1992

Gröbner bases and an application to primary decomposition

Terrie Freni-Johnson
San Jose State University

Order Number 1350081

Gröbner bases and an application to primary decomposition

Freni-Johnson, Terrie Ann, M.S.

San Jose State University, 1992

U·M·I

300 N. Zeeb Rd.
Ann Arbor, MI 48106

GRÖBNER BASES
AND
AN APPLICATION TO PRIMARY DECOMPOSITION

A Thesis

Presented to

The Faculty of the Department of Mathematics

San Jose State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

By

Terrie Freni-Johnson

August, 1992

Approved for the Department of Mathematics

Dr. Eloise Hamann

Dr. Tatiana Shubin

Dr. Ho-Kuen Ng

Approved for the University

Abstract

GRÖBNER BASES
AND
AN APPLICATION TO PRIMARY DECOMPOSITION

by Terrie Freni-Johnson

The purpose of this thesis is to present a detailed explanation of the algorithm stated in Lazard's paper, "Ideal Bases and Primary Decomposition: Case of Two Variables," which utilizes Gröbner bases to compute the primary decomposition of one dimensional ideals in the polynomial ring $K[x, y]$, where K is a field.

Chapter 1 summarizes the general results in commutative algebra which are necessary to prove the effectiveness of Lazard's algorithm. In this chapter, R is assumed to be a commutative ring possessing an identity element.

Chapter 2 provides an exposition of Gröbner bases as described in Robbiano's paper, "Gröbner Bases: A Foundation for Commutative Algebra." This chapter is confined to the polynomial ring $K[x_1, \ldots, x_n]$, where K is a field, and, with a basic knowledge of polynomial rings, is independent of the other chapters.

Chapter 3 presents Lazard's algorithm, an application of Gröbner bases to primary decomposition of ideals in $K[x, y]$.

Acknowledgements

I would like to express my sincere appreciation to Dr. Hamann, my advisor, for her patience and guidance. I especially want to thank her for always being available for questions and never failing to help me understand the answers. I would also like to thank the members of my committee for their many useful suggestions, and Dr. Roger Alperin for supplying a copy of Robbiano's paper. Furthermore, I wish to give special thanks to my husband whose many questions, answers, and suggestions helped to improve this thesis.

Contents

Chapter 1

Preliminaries

In this chapter, we direct our attention to commutative rings which possess an identity element, particularly the special case with $R = K[x_1, \ldots, x_n]$ where K is a field and $x_1, \ldots, x_n$ are indeterminates. Such rings are Noetherian, unique factorization domains, naturally graded, and have Krull dimension n. We include information about these properties and other necessary results for our study of $K[x_1, \ldots, x_n]$.

Most of the theorems and definitions presented in this chapter are found in graduate algebra textbooks. If the proofs are short and self-contained, they will be presented; otherwise, appropriate references will be made.

1.1 Properties of Noetherian Rings

The special class of rings defined below has been named in recognition of the early studies of Emmy Noether. The definition is given in terms of three equivalent conditions, the proof of which can be found in Burton (1970, p. 218).

DEFINITION 1 *A commutative ring R with identity is* **Noetherian** *if it satisfies the following equivalent conditions:*

(i) *For every ascending chain* $\mathcal{U}_1 \subseteq \mathcal{U}_2 \subseteq \mathcal{U}_3 \subseteq \cdots$ *of ideals of* R*, there exists an integer* n *such that* $\mathcal{U}_i = \mathcal{U}_n$ *for all* $i \geq n$*;*

(ii) *every nonempty set of ideals of* R *contains a maximal element;*

(iii) *every ideal* $\mathcal{U}$ *of* R *is finitely generated.*

The finiteness properties of Noetherian rings lead to some useful results, especially in the study of ideals. Every commutative principal ideal domain, hence every field, is a Noetherian ring. Thus, some basic examples of Noetherian rings are $\mathbf{Z}$ and $K[x]$ with K a field. The following theorem, stated and proved in Zariski and Samuel (1958, p. 201), verifies that many examples of Noetherian rings exist.

THEOREM 1.1 (HILBERT'S BASIS THEOREM) *If* R *is a Noetherian ring, then so is any polynomial ring in a finite number of indeterminates over* R*.*

The above theorem affirms that $K[x_1, \ldots, x_n]$ is a Noetherian ring. While $K[x_1, \ldots, x_n]$ is a very special Noetherian ring, it is a source for many more general Noetherian rings since any ring generated over K by n elements is a homomorphic image of $K[x_1, \ldots, x_n]$ and homomorphic images of Noetherian rings are Noetherian. We will see that the equivalent conditions of Definition 1 support the existence of Gröbner bases in $K[x_1, \ldots, x_n]$ as asserted in Chapter 2. Furthermore, the algorithm presented in Chapter 3 is based on a fundamental property of $K[x, y]$ implied from these conditions. We will see that this fundamental result characterizes arbitrary ideals in Noetherian rings in terms of primary ideals which are defined below.

DEFINITION 2 *Let* R *be an arbitrary commutative ring and let* $a, b \in R$*. An ideal* $\mathcal{Q} \neq R$ *of* R *is* **primary** *if whenever* $ab \in \mathcal{Q}$ *and* $a \notin \mathcal{Q}$*, then* $b^n \in \mathcal{Q}$ *for some positive integer* n*.*

EXAMPLE 1.1 The ideal $\langle 4 \rangle$ is a primary ideal of $\mathbf{Z}$.

A stronger notion than a primary ideal is that of a prime ideal.

DEFINITION 3 *Let R be a commutative ring and let $a, b \in R$. An ideal $\mathcal{P}$ of R is* **prime** *if $\mathcal{P} \neq R$ and $ab \in \mathcal{P}$ implies $a \in \mathcal{P}$ or $b \in \mathcal{P}$.*

Clearly, in a commutative ring, every prime ideal is also primary.

EXAMPLE 1.2 The ideal $\langle 2 \rangle$ is a prime ideal of $\mathbf{Z}$ and hence a primary ideal of $\mathbf{Z}$. However, $\langle 4 \rangle$ is not a prime ideal of $\mathbf{Z}$ since $2 \cdot 2 \in \langle 4 \rangle$ but $2 \notin \langle 4 \rangle$.

From the next definition emerges a strong relationship between prime and primary ideals.

DEFINITION 4 *Let $\mathcal{U}$ be an ideal in a commutative ring R. The* **radical** *of $\mathcal{U}$, denoted $\sqrt{\mathcal{U}}$, equals $\{b \in R \mid b^n \in \mathcal{U}$ for some $n \in \mathbf{N}\}$.*

EXAMPLE 1.3 Consider $\langle 72 \rangle$ as an ideal in $\mathbf{Z}$. $\sqrt{\langle 72 \rangle} = \{a \in \mathbf{Z} \mid a^n \in \langle 72 \rangle\} = \langle 6 \rangle$ since $6^3 \in \langle 72 \rangle$ and if $b \in \sqrt{\langle 72 \rangle}$, then $2 \mid b$ and $3 \mid b$.

It turns out that $\sqrt{\mathcal{U}}$ is an ideal containing $\mathcal{U}$. The next theorem looks at the special case where $\mathcal{U}$ is a primary ideal.

THEOREM 1.2 *Let $\mathcal{Q}$ be a primary ideal of a commutative ring R with identity. $\sqrt{\mathcal{Q}}$ is the smallest prime ideal of R which contains $\mathcal{Q}$.*

PROOF Let $\mathcal{Q}$ be a primary ideal of R. First we will verify that $\sqrt{\mathcal{Q}}$ is an ideal containing $\mathcal{Q}$. $\mathcal{Q} \subseteq \sqrt{\mathcal{Q}}$ follows immediately from the definition of $\sqrt{\mathcal{Q}}$. Pick $a, b \in \sqrt{\mathcal{Q}}$. Then $a^n \in \mathcal{Q}$ and $b^m \in \mathcal{Q}$. The binomial theorem implies $(a-b)^{nm} \in \mathcal{Q}$. Hence $a - b \in \sqrt{\mathcal{Q}}$. Furthermore, if $r \in R$, then $ra \in \sqrt{\mathcal{Q}}$ since $(ra)^n = r^n a^n \in \mathcal{Q}$.

To see $\sqrt{\mathcal{Q}}$ is prime, suppose $ab \in \sqrt{\mathcal{Q}}$ and $a \notin \sqrt{\mathcal{Q}}$. Now $(ab)^n = a^n b^n \in \mathcal{Q}$ for some integer n. So $a^n \notin \mathcal{Q}$ since $a \notin \sqrt{\mathcal{Q}}$, but $\mathcal{Q}$ primary implies that there exists an integer m such that $(b^n)^m \in \mathcal{Q}$. Hence $b \in \sqrt{\mathcal{Q}}$. Thus, $\sqrt{\mathcal{Q}}$ is a prime ideal containing $\mathcal{Q}$.

Assume $\mathcal{P}$ is a prime ideal such that $\mathcal{Q} \subseteq \mathcal{P}$ but $\sqrt{\mathcal{Q}} \not\subseteq \mathcal{P}$, then there exists $r \in \sqrt{\mathcal{Q}}$ such that $r \notin \mathcal{P}$. But then $r^n \in \mathcal{Q}$ for some n which implies that $r \in \mathcal{P}$ because P is prime. Therefore, $\sqrt{\mathcal{Q}}$ is the smallest prime ideal containing $\mathcal{Q}$. □

When $\sqrt{\mathcal{Q}} = \mathcal{P}$, where $\mathcal{Q}$ is a primary ideal, it is said that $\mathcal{Q}$ is **$\mathcal{P}$-primary** or that $\mathcal{P}$ is the **associated prime** of $\mathcal{Q}$. Many different primary ideals can be associated with the same prime ideal. For instance, in $\mathbf{Z}$, for any positive integer n, $\langle 2^n \rangle$ is $\langle 2 \rangle$-primary.

The theorem below asserts that the converse of the previous theorem is true under the condition that $\mathcal{P}$ is a maximal ideal.

THEOREM 1.3 *Let $\mathcal{Q}$ and $\mathcal{M}$ be ideals of a communtative ring R with identity and let $\mathcal{M}$ be maximal. If $\sqrt{\mathcal{Q}} = \mathcal{M}$, then $\mathcal{Q}$ is a primary ideal.*

PROOF Suppose $ab \in \mathcal{Q}$ and $a \notin \mathcal{Q}$. We wish to show that $b \in \mathcal{M}$. To achieve a contradiction, suppose $b \notin \mathcal{M}$. Then $\mathcal{M} + \langle b \rangle = R$ since $\mathcal{M}$ is maximal. Therefore, for some $c \in \mathcal{M}$ and $d \in R$,

$$1 = c + bd.$$

Since $\mathcal{M} = \sqrt{\mathcal{Q}}$, there exists an m such that $c^m \in \mathcal{Q}$. The binomial theorem yields

$$1 = 1^m = c^m + bd'$$

where $d' \in R$. Hence, $a = ac^m + abd' \in \mathcal{Q}$. □

The next well-known theorem is a fundamental result on Noetherian rings and is frequently named in honor of Emmy Noether who is responsible for the commonly presented proof found in Zariski and Samuel (1958, p. 209).

THEOREM 1.4 *Every proper ideal of a Noetherian ring can be represented as a finite intersection of primary ideals.*

Therefore, for every ideal $\mathcal{I}$ in a Noetherian ring R, there exists $\{\mathcal{Q}_i \mid i = 1, \ldots, n\}$, a set of primary ideals in R, such that $\mathcal{I} = \cap_{i=1}^{n} \mathcal{Q}_i$. This representation

of $\mathcal{I}$ is termed a **primary decomposition** of $\mathcal{I}$, the $\mathcal{Q}_i$ are called **primary components** of the decomposition, and $\sqrt{\mathcal{Q}_i}$ are referred to as the **associated prime ideals** of $\mathcal{I}$. In the ring of integers, this result is comparable to the Fundamental Theorem of Arithmetic, for in $\mathbf{Z}$, $\langle p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \rangle = \langle p_1^{a_1} \rangle \cap \langle p_2^{a_2} \rangle \cap \cdots \cap \langle p_k^{a_k} \rangle$ where the p_i are distinct primes.

The question remains about the uniqueness of these representations. In general, the $\mathcal{Q}_i$ are not unique; however, unique characteristics of the representation do exist. First it is necessary to introduce the following definiton.

DEFINITION 5 *A primary decomposition $\mathcal{I} = \cap_{i=1}^{n} \mathcal{Q}_i$ is said to be* **irredundant** *if it satisfies the following two conditions:*

(i) *No $\mathcal{Q}_i$ contains the intersection of the other primary components in the decomposition.*

(ii) *The $\mathcal{Q}_i$ have distinct associated prime ideals.*

Any finite primary decomposition $\mathcal{I} = \cap_{i=1}^{n} \mathcal{Q}_i$ can be transformed into an irredundant one by omitting appropriate $\mathcal{Q}_i$'s to achieve *(i)* and, to obtain *(ii)*, setting $\mathcal{Q}'$ equal to the intersection of all those primary components having the same associated prime, since if $\sqrt{\mathcal{Q}_1} = \sqrt{\mathcal{Q}_2}$, then $\sqrt{\mathcal{Q}_1 \cap \mathcal{Q}_2} = \sqrt{\mathcal{Q}_1} = \sqrt{\mathcal{Q}_2}$. The uniqueness of the associated primes which occur in such a representation is given in the theorem below and proved in Zariski and Samuel (1958, p. 211).

THEOREM 1.5 *Let $\mathcal{I}$ be an ideal in a Noetherian ring R such that $\mathcal{I} = \cap_{i=1}^{n} \mathcal{Q}_i$ is an irredundant primary decomposition. The associated prime ideals $\sqrt{\mathcal{Q}_i}$ are uniquely determined by $\mathcal{I}$.*

Thus if $\mathcal{I} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_n = \mathcal{Q}'_1 \cap \cdots \cap \mathcal{Q}'_m$ are two irredundant primary representations of $\mathcal{I}$, then $m = n$ and the $\mathcal{Q}_i$ can be renumbered so that $\sqrt{\mathcal{Q}_i} = \sqrt{\mathcal{Q}'_i}$. However, it is not necessarily the case that $\mathcal{Q}_i = \mathcal{Q}'_i$.

EXAMPLE 1.4 Consider the ideal $\mathcal{I} = \langle x^2, yx \rangle$ in the Noetherian ring $\mathbf{R}[x, y]$.

$$\mathcal{I} = \langle x^2, y \rangle \cap \langle x \rangle \quad \text{and} \quad \mathcal{I} = \langle x^2, xy, y^3 \rangle \cap \langle x \rangle$$

are both irredundant primary representations for $\mathcal{I}$. Notice $\langle x^2, y \rangle \neq \langle x^2, xy, y^3 \rangle$, but $\sqrt{\langle x^2, y \rangle} = \sqrt{\langle x^2, xy, y^3 \rangle} = \langle x, y \rangle$.

In an irredundant primary representation for $\mathcal{I}$, an associated prime ideal $\mathcal{P}$ of $\mathcal{I}$ is said to be **isolated** if $\mathcal{P}$ is a minimal element in the set of associated prime ideals of $\mathcal{I}$, otherwise, $\mathcal{P}$ is termed **embedded.** A primary component $\mathcal{Q}$ of $\mathcal{I}$ is referred to as embedded or isolated in correspondence to the associated prime ideal $\sqrt{\mathcal{Q}_i}$. In Example 1.4, $\langle x \rangle$ is the only isolated prime ideal for $\langle x^2, xy \rangle$, and $\langle x, y \rangle$ is embedded.

We now characterize the isolated prime ideals of a primary decomposition.

THEOREM 1.6 *Let $\mathcal{I}$ be an ideal in a Noetherian ring R. $\mathcal{P}$ is an isolated prime ideal of $\mathcal{I}$ if and only if $\mathcal{P}$ is minimal in the set of prime ideals containing $\mathcal{I}$.*

PROOF Let $\mathcal{I} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_n$ be an irredundant primary decomposition for $\mathcal{I}$, and for each i, $\mathcal{P}_i = \sqrt{\mathcal{Q}_i}$. Suppose $\mathcal{P}_k$ is an isolated prime of $\mathcal{I}$ and let $\mathcal{P}$ be a prime ideal such that

$$\mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_n = \mathcal{I} \subseteq \mathcal{P} \subseteq \mathcal{P}_k.$$

Since P is prime, there exists at least one $t \leq n$ such that $\mathcal{Q}_t \subseteq \mathcal{P}$, otherwise for every $i \leq n$ there is an element q_i of $\mathcal{Q}_i$ such that $q_i \notin \mathcal{P}$ which implies $q_1 \cdots q_n$ is an element of $\mathcal{I}$ which does not lie in $\mathcal{P}$. In fact, $\sqrt{\mathcal{Q}_t} \subseteq \mathcal{P}$ as implied by Theorem 1.2, and since $\mathcal{P}_k$ is an isolated prime of $\mathcal{I}$, $\sqrt{\mathcal{Q}_t} = \mathcal{P} = \mathcal{P}_k$. Hence $\mathcal{P}_k$ is a minimal prime.

Conversely, assume $\mathcal{P}$ is minimal in the set of prime ideals containing $\mathcal{I}$. It suffices to show that $\mathcal{P}$ is an associated prime of the above irredundant decomposition of $\mathcal{I}$. Since $\mathcal{I} \subseteq \mathcal{P}$, $\mathcal{P}$ must contain $\sqrt{\mathcal{Q}_j}$ for some $j \leq n$, as shown above. But since $\mathcal{P}$ is minimal it must be the case that $\mathcal{P} = \sqrt{\mathcal{Q}_j}$. □

The theorem below proved in Zariski and Samuel (1958, p. 212) is essential to the proof of the Algorithm presented in Chapter 3.

THEOREM 1.7 *Let R be a Noetherian ring, and let $\mathcal{I}$ be an ideal of R such that $\mathcal{I} = \cap_{i=1}^{n} \mathcal{Q}_i$ is an irredundant primary decomposition. The isolated primary components of $\mathcal{I}$ are uniquely determined by $\mathcal{I}$.*

The next result follows immediately from the above theorem.

COROLLARY 1 *Let $\mathcal{I}$ be an ideal of a Noetherian ring R such that $\mathcal{I}$ has no embedded components. Then $\mathcal{I}$ has a unique primary decomposition.*

The reader may wish to note that the lack of uniqueness in Example 1.4 occurred only in the case of the embedded primary component corresponding to the embedded prime $\langle x, y \rangle$. In the next section, we will look at a class of ideals which satisfy the condition of possessing no embedded primes, and thus admit unique primary decompositions.

1.2 Miscellaneous Results

This section summarizes some basic results about dimension of ideals, localization at prime ideals, graded rings, and primitive polynomials. Unless otherwise specified, the reader should assume that R is a commutative ring with an identity element.

DEFINITION 6 *Let $\mathcal{P}$ be a prime ideal in a ring R. $\mathcal{P}$ is said to be of* **rank** *n, denoted rank$\mathcal{P} = n$, if there exists a strictly descending chain*

$$\mathcal{P} \supset \mathcal{P}_1 \supset \mathcal{P}_2 \supset \cdots \supset \mathcal{P}_n$$

of prime ideals and no longer such chain of prime ideals exists.

In a Noetherian ring, $\operatorname{rank}\mathcal{P}$ will always be finite. When $\mathcal{I}$ is an arbitrary proper ideal in a ring R, $\operatorname{rank}\mathcal{I} = \inf\{\operatorname{rank}\mathcal{P} \mid \mathcal{P} \text{ is prime and } \mathcal{P} \supseteq \mathcal{I}\}$. Rank is sometimes termed *height* as it can be thought of as a measurement of distance of $\mathcal{P}$ from the bottom of a maximal ideal. Similarly, dimension, defined below, is sometimes referred to as *depth* as it measures length from the top of a chain down to the ideal in question.

DEFINITION 7 *Let $\mathcal{P}$ be a prime ideal in a ring R. $\mathcal{P}$ is of* **dimension** *n, denoted $\dim\mathcal{P} = n$, if there exists a strictly ascending chain*

$$\mathcal{P} \subset \mathcal{P}_1 \subset \mathcal{P}_2 \subset \cdots \subset \mathcal{P}_n$$

of prime ideals and no longer such chain of prime ideals exists.

If $\mathcal{I}$ is an arbitrary proper ideal, then $\dim\mathcal{I} = \sup\{\dim\mathcal{P} \mid \mathcal{P} \supseteq \mathcal{I}\}$. Notice it is always the case that the maximal ideals of R have dimension zero. If, in R, there exists at least one strictly increasing sequence $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \mathcal{P}_2 \subset \cdots \subset \mathcal{P}_n$ of prime ideals and no longer such chain of prime ideals exists, then R is said to be of dimension n or to have Krull dimension n, denoted $\dim R = n$. If R is a Noetherian domain, in the chain above, $\mathcal{P}_0 = \langle 0\rangle$, $\mathcal{P}_n$ is a maximal ideal. Note that $\dim\langle 0\rangle = \max\{\operatorname{rank}\mathcal{M} \mid \mathcal{M} \text{ is a maximal ideal of } R\}$.

The theorem below, proved in Northcott (1968, p. 282), states that in a polynomial ring over a field, the rank of the maximal ideals depends on the number of indeterminates.

THEOREM 1.8 *Let K be a field and $\mathcal{M}$ a maximal ideal of $K[x_1, \ldots, x_n]$. Then $\operatorname{rank}\mathcal{M} = n$, and $\mathcal{M}$ can be generated by n elements.*

EXAMPLE 1.5 For any field K, $\dim K[x, y] = 2$. $\langle 0\rangle \subset \langle x\rangle \subset \langle x, y\rangle$ is a chain of prime ideals of length two. Notice $\langle 0\rangle$ is the only two dimensional ideal in $K[x, y]$.

THEOREM 1.9 *In a unique factorization domain, D, all rank one prime ideals are principal.*

PROOF Let D be a unique factorization domain. Let $\mathcal{P}$ be a prime ideal in D such that $\operatorname{rank}\mathcal{P} = 1$. Note $\mathcal{P} \neq \langle 0 \rangle$ and since $\operatorname{rank}\mathcal{P} = 1$ and D is an integral domain, $\langle 0 \rangle$ is the only prime ideal properly contained in $\mathcal{P}$. Suppose r is a nonzero element of $\mathcal{P}$, then since D is a unique factorization domain, $r = i_1 \cdots i_k$ where each i_j is irreducible. Since $\mathcal{P}$ is prime, there exists j such that $i_j \in \mathcal{P}$ and $\langle i_j \rangle$ is a prime ideal contained in $\mathcal{P}$. Hence $\langle i_j \rangle = \mathcal{P}$. □

COROLLARY 2 *In $K[x,y]$, where K is a field, all dimension one prime ideals are principal.*

PROOF Suppose $\mathcal{P}$ is a one dimensional prime ideal of $K[x,y]$, then there exists a maximal ideal $\mathcal{M}$ of $K[x,y]$ such that $\mathcal{P} \subset \mathcal{M}$ and no such longer strictly ascending chain of prime ideals exists. Since $\dim K[x,y] = 2$, $\operatorname{rank}\mathcal{P} = 2$ or 1. If $\operatorname{rank}\mathcal{P} = 2$, then $\dim\mathcal{P} = 0$. Therefore, $\operatorname{rank}\mathcal{P} = 1$, and Theorem 1.9 implies $\mathcal{P}$ is a principal ideal. □

COROLLARY 3 *In $K[x,y]$, where K is a field, all nonzero prime ideals are either principal or maximal.*

PROOF Theorem 1.8 implies $\dim K[x,y] = 2$. Thus, any nonzero prime ideal $\mathcal{P}$ is of dimension zero or of dimension one. Therefore, $\mathcal{P}$ is either maximal, or by Corollary 2, $\mathcal{P}$ is principal. □

COROLLARY 4 *Let $\langle 0 \rangle \neq \mathcal{I} = \langle f_0, \ldots, f_k \rangle \neq K[x,y]$ with $f_0, \ldots, f_k \in K[x,y]$ where K is a field.* $\operatorname{Gcd}\{f_i\} = 1$ *if and only if $\dim\mathcal{I} = 0$.*

PROOF Assume $\gcd\{f_i\}$. Since $\langle 0 \rangle \neq \mathcal{I}$, then $\dim\mathcal{I} = 1$ or 0. If $\dim\mathcal{I} = 1$, then there exists a prime ideal $\mathcal{P}$ such that $\mathcal{I} \subseteq \mathcal{P}$ and $\dim\mathcal{P} = 1$. Then Corollary 2 implies that $\mathcal{P}$ is a principal ideal, and hence $\mathcal{I} = \langle q \rangle$ for some $q \in K[x,y]$. Therefore, $q \mid f_i$ for every $i = 0, \ldots, k$, which contradicts $\gcd\{f_i\} = 1$. Thus, $\dim\mathcal{I} = 0$.

Let $\dim \mathcal{I} = 0$, and to obtain a contradiction, assume $\gcd\{f_i\} \neq 1$. Then there exists d, an irreducible element of $K[x,y]$ such that $d \mid f_i$ for every $i = 0, \ldots, k$. Note that $\langle d \rangle$ is a prime ideal containing $\mathcal{I}$, and since $\dim \mathcal{I} = 0$, $\langle d \rangle$ is a maximal ideal. Thus Theorem 1.8 implies $\operatorname{rank} \langle d \rangle = 2$, but there does not exist a nonzero prime ideal properly contained in $\langle d \rangle$ since d is irreducible. □

It's important to note that the only prime ideals containing a dimension zero ideal are maximal ideals. Therefore, in a Noetherian ring, dimension zero ideals have only maximal ideals occurring as associated prime ideals and thus their decompositions will not contain embedded primary ideals. In other words, in Noetherian rings, dimension zero ideals can be uniquely represented as an intersection of primary ideals. In particular, an ideal of $K[x,y]$ has a unique primary decomposition if its generating set has no common divisors, and our main algorithm is designed especially for these ideals of $K[x,y]$. The proof of this algorithm essentially depends on certain results related to localization described below.

DEFINITION 8 *Let R be an integral domain and $\mathcal{P}$ a prime ideal of R. $R_{\mathcal{P}} = \{\frac{a}{s} \mid a \in R \text{ and } s \in R \setminus \mathcal{P}\}$ is the* **localization of R at $\mathcal{P}$**.

Note that, in $R_{\mathcal{P}}$, all of the elements not in $\mathcal{P}$ become invertible and $\frac{a}{s} = as^{-1}$. $R_{\mathcal{P}}$ is often referred to as the ring of quotients of R with respect to $\mathcal{P}$. A more general case of localization is the ring of quotients of R with respect to S, where S is any multiplicatively closed subset of R, not necessarily the complement of a prime ideal, and $R_S = \{as^{-1} \mid a \in R, s \in S\}$. If $\mathcal{I}$ is any ideal of R, $\mathcal{I}_{\mathcal{P}} = S^{-1}\mathcal{I} = \langle \{bs^{-1} \mid b \in \mathcal{I},\ s \in S\} \rangle$ is an ideal of $R_{\mathcal{P}}$ where $S = R \setminus \mathcal{P}$.

The localization of R at a prime ideal $\mathcal{P}$ creates a local ring $R_{\mathcal{P}}$, a ring which contains only one maximal ideal, $\mathcal{P}_{\mathcal{P}}$. Considering the localization of an ideal $\mathcal{I}$ at a prime $\mathcal{P}$ can be a useful tool in discovering certain properties of $\mathcal{I}$, as we will see in Chapter 3 where the next two theorems will be utilized.

THEOREM 1.10 *Let $\mathcal{Q}$ be a primary ideal of R where $\sqrt{\mathcal{Q}} = \mathcal{P}$. If $\bar{\mathcal{P}}$ is a prime ideal of R, then the following hold:*

(i) *If $\mathcal{P} \not\subseteq \bar{\mathcal{P}}$, then $\mathcal{P}_{\bar{\mathcal{P}}} = \mathcal{Q}_{\bar{\mathcal{P}}} = R_{\bar{\mathcal{P}}}$.*

(ii) *If $\mathcal{P} \subseteq \bar{\mathcal{P}}$, then $\mathcal{P}_{\bar{\mathcal{P}}} \cap R = \mathcal{P}$ and $\mathcal{Q}_{\bar{\mathcal{P}}} \cap R = \mathcal{Q}$.*

PROOF *(i)* If $\mathcal{P} \not\subseteq \bar{\mathcal{P}}$, then there exists an $a \in \mathcal{P}$ such that $a \notin \bar{\mathcal{P}}$. Thus, $a^n \notin \bar{\mathcal{P}}$ for all n which implies $\mathcal{Q} \not\subseteq \bar{\mathcal{P}}$. And $1 = \frac{a}{a} = \frac{a^n}{a^n} \in \mathcal{Q}_{\bar{\mathcal{P}}} \subseteq \mathcal{P}_{\bar{\mathcal{P}}}$. Hence $\mathcal{Q}_{\bar{\mathcal{P}}} = \mathcal{P}_{\bar{\mathcal{P}}} = R_{\bar{\mathcal{P}}}$.

(ii) Suppose $\mathcal{P} \subseteq \bar{\mathcal{P}}$. It suffices to show that the second equality holds since the first is the special case where $\mathcal{P} = \mathcal{Q}$. Choose $b \in \mathcal{Q}_{\bar{\mathcal{P}}} \cap R$. So $b = \frac{q}{s}$ where $q \in \mathcal{Q}$ and $s \notin \bar{\mathcal{P}}$. Hence $s \notin \mathcal{P}$ and $bs \in \mathcal{Q}$. It follows that $b \in \mathcal{Q}$ since otherwise a power of s is in $\mathcal{Q}$ which contradicts $s \notin \mathcal{P}$. Therefore, $\mathcal{Q} \supseteq \mathcal{Q}_{\bar{\mathcal{P}}} \cap R$ and hence $\mathcal{Q} = \mathcal{Q}_{\bar{\mathcal{P}}} \cap R$ since the other inclusion is obvious. □

THEOREM 1.11 *Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ be primary ideals of R. If $\mathcal{P}$ is a prime ideal of R, then $(\mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_n)_{\mathcal{P}} = (\mathcal{Q}_1)_{\mathcal{P}} \cap \cdots \cap (\mathcal{Q}_n)_{\mathcal{P}}$.*

PROOF Let $\mathcal{I} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_n$, and renumber the $\mathcal{Q}_i$ so that for $i \leq r$, $\sqrt{\mathcal{Q}_i} \subseteq \mathcal{P}$, and for $i > r$, $\sqrt{\mathcal{Q}_i} \not\subseteq \mathcal{P}$. Then, by Theorem 1.10, $(\mathcal{Q}_i)_{\mathcal{P}} \cap R = \mathcal{Q}_i$ for $i \leq r$, and $(\mathcal{Q}_i)_{\mathcal{P}} = R_{\mathcal{P}}$ for $i > r$. Note that for every i, $\mathcal{I}_{\mathcal{P}} \subseteq (\mathcal{Q}_i)_{\mathcal{P}}$. Thus

$$\mathcal{I}_{\mathcal{P}} \subseteq (\mathcal{Q}_1)_{\mathcal{P}} \cap \cdots \cap (\mathcal{Q}_n)_{\mathcal{P}} = (\mathcal{Q}_1)_{\mathcal{P}} \cap \cdots \cap (\mathcal{Q}_r)_{\mathcal{P}}.$$

Pick $b \in (\mathcal{Q}_1)_{\mathcal{P}} \cap \cdots \cap (\mathcal{Q}_r)_{\mathcal{P}}$ and let $b = \frac{a}{s}$ where $a \in R$ and s is invertible in $R_{\mathcal{P}}$. Then for every $i \leq r$, $a \in s(\mathcal{Q}_i)_{\mathcal{P}} = (\mathcal{Q}_i)_{\mathcal{P}}$ and since $(\mathcal{Q}_i)_{\mathcal{P}} \cap R = \mathcal{Q}_i$, $a \in \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_r$. Let $s_{r+1}, \ldots, s_n \in R \setminus \mathcal{P}$ so that $s_{r+j} \in \mathcal{Q}_{r+j}$. Then $a' = as_{r+1} \cdots s_n \in \mathcal{I}$, and $b = \frac{a}{s} = \frac{a'}{ss_{r+1} \cdots s_n} \in \mathcal{I}_{\mathcal{P}}$. Hence $\mathcal{I}_{\mathcal{P}} = (\mathcal{Q}_1)_{\mathcal{P}} \cap \cdots \cap (\mathcal{Q}_n)_{\mathcal{P}}$. □

Note that in the two proofs above, the fact that we are localizing at a prime ideal, or rather at the complement of a prime ideal, instead of at an arbitrary

multiplicatively closed subset of R, is not used. In fact, these two theorems and proofs are found in Nagata (1962, p. 16) and are stated in this more general case.

In Chapter 2, it is necessary to fix an additional structure on $K[x_1, \ldots, x_n]$ and hence we introduce the theory of a graded ring.

DEFINITION 9 *Let R be a commutative ring with an identity element. A* **Γ-grading** *on R is a family $\{R_{(\gamma)}\}_{\gamma \in \Gamma}$ of subgroups of $(R, +)$ such that*

(i) $R = \sum_{\gamma \in \Gamma} R_{(\gamma)}$ *(direct sum);*

(ii) $R_{(\gamma)} R_{(\gamma')} \subseteq R_{(\gamma+\gamma')}$ *for every $\gamma, \gamma' \in \Gamma$.*

For every $\gamma \in \Gamma$, the elements of $R_{(\gamma)}$ are said to be **homogeneous** of degree γ. If R is a graded ring, the above definition can be generalized to any R-module.

DEFINITION 10 *Let $R = \sum_{\gamma \in \Gamma} R_{(\gamma)}$ be a Γ-graded ring and let E be an R-module. A* **Γ-grading** *on E is a family $\{E_{(\gamma)}\}_{\gamma \in \Gamma}$ of subgroups of $(E, +)$ which satisfies*

(i) $E = \sum_{\gamma \in \Gamma} E_{(\gamma)}$ *(direct sum);*

(ii) $R_{(\gamma)} E_{(\gamma')} \subseteq E_{(\gamma+\gamma')}$ *for all $\gamma, \gamma' \in \Gamma$.*

The example below illustrates a grading on a general polynomial ring. The reader should note that $\mathbf{N}$ represents the set of natural numbers, $\mathbf{Z}$ represents the set of integers, and $\mathbf{R}$ represents the set of real numbers.

EXAMPLE 1.6 For every $n \in \mathbf{N}$, the ring $A = R[x_1, \cdots, x_n]$, where R is any ring, is naturally graded with the $\mathbf{Z}^n$ -grading, by setting $A_{(a_1,\ldots,a_n)} = \{c x_1^{a_1} \cdots x_n^{a_n} \mid c \in R\}$. If $n = 3$ and $R = \mathbf{R}$, then $4x^2y^3z^7$ is a homogeneous element of degree $(2, 3, 7)$.

The following definition and proposition are needed to develop the structure of certain Gröbner bases in Chapter 3. They are stated here for any unique factorization domain D; however, they will be utilized in the special case $D = K[x]$ where K is a field. Recall that if D is a unique factorization domain, then so is $D[x]$ and thus $D[x_1, \ldots, x_n]$.

DEFINITION 11 *Let D be a unique factorization domain. A polynomial f in $D[x]$ is said to be* **primitive** *if the greatest common factor of the coefficients of f is a unit in D.*

PROPOSITION 1 *Let D be a unique factorization domain and $f(x), g(x) \in D[x]$. If $g(x) \mid bf(x)$ where $b \in D$ and $g(x)$ is primitive in $D[x]$, then $g(x)$ divides $f(x)$.*

The reader is referred to Zariski and Samuel (1958, p. 33) for the proof of the above proposition.

We now have all the preliminary material necessary to develop the algorithm presented in Robbiano (p.44) which computes a Gröbner basis for ideals in $K[x_1, \ldots, x_n]$ and the algorithm presented in Lazard (1985, p. 265) which computes the primary decomposition of one dimensional ideals in $K[x, y]$.

Chapter 2

Gröbner Bases

The study of Gröbner bases is confined to polynomial rings, $A = K[x_1, \ldots, x_n]$, where K is a field. Ideals in A can generally be described by a finite generating set of polynomials, called a basis. It can be shown that any finite generating set of an ideal $\mathcal{I}$ can be algorithmically transformed into a Gröbner basis for $\mathcal{I}$. The algorithmic approach to Gröbner bases involves a decision process in which it is necessary to fix a total ordering $<_T$ on monic monomials in A which satisfies the following two conditions:

Let s, t and u be monic monomials in A,

(T1) $1 <_T t$ for all $t \neq 1$;

(T2) if $s <_T t$, then $s \cdot u <_T t \cdot u$.

The reader may assume that an arbitrary total ordering satisfying (T1) and (T2) has been fixed.

2.1 Gröbner Basis Definition and Equivalences

The following definition fixes notation relating to Gröbner bases.

DEFINITION 1 *Let f be nonzero with $f \in A = K[x_1, \ldots, x_n]$ and $\mathcal{I} \neq \langle 0 \rangle$ be an ideal in A.*

(i) $\mathcal{T}=\{x_1^{a_1} \cdots x_n^{a_n} \mid a_i$ *is a natural number*$\}$ *denotes the set of* **terms** *of A which are monic monomials.*

(ii) $lt(f) \in \mathcal{T}$ *denotes the* **leading term** *of f which is the maximal term of f with respect to $<_T$.*

(iii) $lc(f) \in K$ *denotes the* **leading coefficient** *of f, that is the coefficient of $lt(f)$.*

(iv) $lm(f) = lc(f) \cdot lt(f)$ *denotes the* **leading monomial** *of f with respect to $<_T$.*

(v) $coef(f, T) \in K$ *denotes the* **coefficient of the term** *T in f.*

(vi) $lt(\mathcal{I})$ *denotes the* **leading term ideal** *of $\mathcal{I}$ with respect to $<_T$ and is the ideal generated by $\{lt(f) \mid f \in \mathcal{I} \setminus \{0\}\}$.*

(vii) $deg(f)$ *denotes the* **degree** *of f which is the sequence of natural numbers, $(a_1, \ldots, a_n)$, where $lt(f) = x_1^{a_1} \cdots x_n^{a_n}$. For $g \in A$, we say $deg(g) > deg(f)$ if $lt(g) >_T lt(f)$.*

We are now ready to present one definition of a Gröbner basis.

DEFINITION 2 *Let $F = \{f_1, f_2, \ldots, f_t\} \subseteq A \setminus \{0\}$ and $\mathcal{I} = \langle f_1, f_2, \ldots, f_t \rangle$. F is a* **Gröbner basis** *for $\mathcal{I}$ if $\langle lt(f_1), lt(f_2), \ldots, lt(f_t) \rangle = lt(\mathcal{I})$.*

The proposition below verifies that a Gröbner basis exists for any ideal in the polynomial ring A.

PROPOSITION 1 *Let $\mathcal{I} \neq \langle 0 \rangle$ be a proper ideal of $A = K[x_1, \ldots, x_n]$ where K is a field. Then there exists a Gröbner basis for $\mathcal{I}$.*

PROOF Let $\mathcal{I}$ be an ideal of A. Since A is a Noetherian ring, $\mathcal{I}$ is finitely generated, and there exists $\{f_1, f_2, \ldots, f_r\} \subseteq A \setminus \{0\}$ such that

$$\mathcal{I} = \langle f_1, f_2, \ldots, f_r \rangle.$$

Assume that there does *not* exist a Gröbner basis for $\mathcal{I}$. Thus,

$$\mathrm{lt}(\mathcal{I}) \not\subseteq \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_r) \rangle,$$

and so there exists a nonzero $f_{r+1} \in \mathcal{I}$ such that $\mathrm{lt}(f_{r+1}) \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_r) \rangle$, and $\{f_1, f_2, \ldots, f_{r+1}\}$ is not a Gröbner basis for $\mathcal{I}$. Continue this process so that at the i-th step we get

$$f_{r+i} \in \mathcal{I} \quad \text{and} \quad \mathrm{lt}(f_{r+i}) \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_{r+i-1}) \rangle.$$

Let $H_i = \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_{r+i}) \rangle$ for $i = 1, 2, \ldots$, then consider the ascending chain of ideals in A,

$$H_0 \subseteq H_1 \subseteq \cdots \subseteq H_i \subseteq \cdots$$

which does not stabilize. But this contradicts that A is Noetherian. □

In order to decide whether F is a Gröbner basis for the ideal it generates, it is necessary to consider the total ordering assigned to the monic monomials of the ring. In the examples below, assume the monic monomials of A are ordered according to the *pure lexicographical ordering* (where "pure" means $x < y$):

$$1 < x < x^2 < \cdots < y < xy < x^2y < \cdots < y^2 < xy^2 < \cdots.$$

EXAMPLE 2.1 Consider $F = \{x, y\} \subseteq A = K[x, y]$ and let $\mathcal{I} = \langle x, y \rangle$. Since $\mathrm{lt}(\mathcal{I}) = \langle x, y \rangle$, F is a Gröbner basis for $\mathcal{I}$.

In the next example, we look at a different generating set for $\mathcal{I} = \langle x, y \rangle$.

EXAMPLE 2.2 Let $H = \{y + x, y\} \subseteq A = K[x, y]$ and $\mathcal{I} = \langle y + x, y\rangle = \langle x, y\rangle$. H is not a Gröbner basis for $\mathcal{I}$ because $\mathrm{lt}(\mathcal{I}) = \langle x, y\rangle \not\subseteq \langle y\rangle$. In other words, the leading term ideal does not equal the ideal generated by the leading terms of H.

The reader should note that in Example 2.2 if the monic monomials of A were given the *reverse lexicographical ordering*:

$$1 < y < y^2 < \cdots < x < xy < xy^2 < \cdots < x^2 < x^2y < \cdots,$$

then H would in fact be a Gröbner basis for $\mathcal{I}$. So the property of being a Gröbner basis is dependent upon the total ordering.

Futhermore, with respect to the reverse lexicographical ordering, F of Example 2.1, as well as H, is a Gröbner basis for $\mathcal{I} = \langle x, y\rangle$. And so we see that a Gröbner basis for an ideal is not always unique.

Given an arbitrary generating set of nonzero polynomials, $F = \{f_1, f_2, \ldots, f_t\}$, for $\mathcal{I}$, it is always the case that $\mathrm{lt}(F) = \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_t)\rangle \subseteq \mathrm{lt}(\mathcal{I})$. Therefore, the transformation of F into a Gröbner basis is achieved by adjoining to F additional polynomials, $\{f_{t+1}, \ldots, f_s\}$, from $\mathcal{I}$ in order to guarantee that $\mathrm{lt}(\mathcal{I}) \subseteq \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_s)\rangle$. The decision process utilizes Definition 1 as well as other characteristics of Gröbner bases which depend on the next two definitions found in Robbiano (p. 33).

DEFINITION 3 *Let $f, g \in K[x_1, \ldots, x_n]$ and $F = \{f_1, f_2, \ldots, f_t\}$. f* **rewrites (reduces) to** *g* **via** *F, or g is a* **rewriting** *of f, denoted $f \mathrm{R}_F g$, if there exists $f_i \in F$ and $T \in \mathcal{T}$ such that $g = f - \frac{c_i}{\mathrm{lc}(f_i)} \cdot T \cdot f_i$ where $c_i = coef(f, T \cdot lt(f_i))$.*

Note that when $f \mathrm{R}_F g$, with $g \neq f$, it is the case that there exists $f_i \in F$ for which $\mathrm{lt}(f_i)$ divides some term of f, and then T is chosen so that the term $T \cdot \mathrm{lt}(f_i)$ is eliminated from f to get g. In general, $\mathrm{lt}(g) \leq_T \mathrm{lt}(f)$; however, the most interesting case is when the leading term of f is a multiple of $\mathrm{lt}(f_i)$ for some f_i in F, and T is picked so that $\mathrm{lt}(f) = T \cdot \mathrm{lt}(f_i)$ leaving $\mathrm{lt}(g) <_T \mathrm{lt}(f)$.

Transforming F into a Gröbner basis for $\mathcal{I}$ usually requires a series of these reductions, and therefore we adopt the following notation.

DEFINITION 4 *Let* $f, g \in K[x_1, \ldots, x_n]$. *Write* $f \xrightarrow{F} g$ *if there exists* $\{g_0, g_1, \ldots, g_r\} \subset K[x, y]$ *such that* $g_0 = f \mathrm{R_F} g_1, g_1 \mathrm{R_F} g_2, \ldots, g_{r-1} \mathrm{R_F} g_r = g$.

It is important to note that $f = h_0 \xrightarrow{F} h_1 \xrightarrow{F} \cdots \xrightarrow{F} h_r \xrightarrow{F} \cdots$ always stabilizes. In other words, given any polynomial f in A, there exists an h from A for which $f \xrightarrow{F} h$ while there is no h' different from h such that $h \xrightarrow{F} h'$. A useful case occurs when $h = 0$.

REMARK 1 *If* $f \xrightarrow{F} 0$, *then for* $j = 1, 2, \ldots, m$ *there exists* $p_j \in F$, $T_j \in \mathcal{T}$, *and* $c_j \in K$ *so that*

$$0 = f - \sum_{j=1}^{m} \frac{c_j}{lc(p_j)} \cdot T_j \cdot p_j,$$

and for all $j = 1, \ldots, m-1$, $T_{j+1} \cdot lt(p_{j+1}) <_T T_j \cdot lt(p_j)$ *and* $T_1 \cdot lt(p_1) = lt(f)$.

To see this, note that $f \xrightarrow{F} 0$ implies

$$f = h_0 \xrightarrow{F} h_1 \xrightarrow{F} \cdots \xrightarrow{F} h_m = 0$$

where

$$h_j = h_{j-1} - \frac{c_j}{\mathrm{lc}(p_j)} \cdot T_j \cdot p_j \tag{2.1}$$

with $T_j \in \mathcal{T}$, $p_j \in F$, $c_j = \mathrm{coef}(h_{j-1}, T_j \cdot \mathrm{lt}(p_j))$, and $h_{m-1} \neq 0$. In fact, T_j and p_j can be picked so that at each reduction the degree of h_j decreases; that is, for all $j = 1, \ldots, m$, there exists $T_j \in \mathcal{T}$ and $p_j \in F$ so that $T_j \cdot \mathrm{lt}(p_j) = \mathrm{lt}(h_{j-1}) >_T \mathrm{lt}(h_j) = T_{j+1} \cdot \mathrm{lt}(p_{j+1})$. Otherwise, there exists $r < m$ such that for every $T \in \mathcal{T}$ and $p \in F$, $\mathrm{lt}(h_r) \neq T \cdot \mathrm{lt}(p)$ which means $\mathrm{lt}(h_r) = \mathrm{lt}(h_{r+1}) = \cdots = \mathrm{lt}(h_m)$, but this contradicts $h_m = 0$. Then, back substitution in Equation 2.1 yields the result.

In the following examples, the terms of A are ordered according to the pure lexicographical ordering.

EXAMPLE 2.3 Let $F = \{f_1, f_2\}$ where $f_1 = x$ and $f_2 = y$. Consider $f = xy^2 + x^2$. Now $f \xrightarrow{F} x^2$ because $x^2 = f - xy \cdot f_2$ and $x^2 \xrightarrow{F} 0$ because $0 = x^2 - x \cdot f_1$. Therefore, $f \xrightarrow{F} 0$.

The next example, when contrasted with Example 2.3 above, shows that reduction to zero depends on the reducing set, F.

EXAMPLE 2.4 Let $H = \{h_1, h_2\}$ where $h_1 = y + x$ and $h_2 = y$. Consider $f = xy^2 + x^2$. Now $f \xrightarrow{H} x^2$ since $x^2 = f - xy \cdot h_2$, but $x^2 \not\xrightarrow{H} 0$ because x^2 is not a multiple of $\mathrm{lt}(h_1)$ or of $\mathrm{lt}(h_2)$.

A generating set F is in fact a Gröbner basis for $\mathcal{I}$ iff every polynomial in $\mathcal{I}$ reduces to 0 via F. We formally state this fact in Theorem 2.1 below.

THEOREM 2.1 *Let $F = \{f_1, f_2, \ldots, f_t\} \subseteq A \setminus \{0\} = K[x_1, \ldots, x_n] \setminus \{0\}$, where K is a field. Suppose $\mathcal{I} = \langle f_1, f_2, \ldots, f_t \rangle$. The following are equivalent:*

(i) *F is a Gröbner basis for $\mathcal{I}$;*

(ii) *if $f \in \mathcal{I} \setminus \{0\}$, then there exists $g_1, \ldots, g_t \in A$ such that $f = \sum_{j=1}^{t} g_j f_j$ where for each j, $lt(f) \geq_T lt(g_j) \cdot lt(f_j)$, which implies that there exists $i \leq t$ such that $lt(f) = lt(g_i) \cdot lt(f_i)$;*

(iii) *$f \in \mathcal{I}$ iff $f \xrightarrow{F} 0$.*

PROOF First we verify the implication in *(ii)*. Let $f \in \mathcal{I} \setminus \{0\}$ so that for some $g_1, \ldots g_t \in A$, $f = \sum_{j=1}^{t} g_j f_j$ where for all j, $\mathrm{lt}(f) \geq_T \mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)$. Therefore,

$$\mathrm{lt}(f) \geq_T \max\{\mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)\}.$$

However, it is also the case that

$$\mathrm{lt}(f) \leq_T \max\{\mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)\}.$$

Hence, there exists $i \leq t$ such that

$$\mathrm{lt}(f) = \mathrm{lt}(g_i) \cdot \mathrm{lt}(f_i) = \max\{\mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)\}.$$

(i⇒ii) Suppose not. Pick $f \in \mathcal{I} \setminus \{0\}$ least for which *(ii)* does not hold. By hypothesis, $\mathrm{lt}(f) \in \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_t) \rangle$ Therefore, there exist $c_i \in K$ and $T_i \in \mathcal{T}$ so that

$$\mathrm{lt}(f) = \sum_{f_j \in F} c_j T_j \cdot \mathrm{lt}(f_j).$$

Since $\mathrm{lt}(f) \in \mathcal{T}$, it cannot equal a sum of terms so there exists a $T \in \mathcal{T}$ and $k \leq t$ such that $\mathrm{lt}(f) = T \cdot \mathrm{lt}(f_k)$. It follows that there exists a $c \in K$ with $\mathrm{lt}(f - cTf_k) <_T \mathrm{lt}(f)$. By the choice of f,

$$f - cTf_k = \textstyle\sum_{j=1}^{t} g_j f_j,$$

where $\mathrm{lt}(f - cTf_k) \geq_T \mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)$ for all j. Then

$$f = \textstyle\sum_{j=1}^{t} g_j f_j + cTf_k$$

where $\mathrm{lt}(f) \geq_T \mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)$ for all j, which contradicts the assumption.

(ii⇒i) Let $h \in \mathrm{lt}(\mathcal{I}) \setminus \{0\}$, then

$$h = \sum_{i=1}^{l} p_i \cdot \mathrm{lt}(h_i) \tag{2.2}$$

where $h_i \in \mathcal{I} \setminus \{0\}$ and $p_i \in A$. Fix $i \leq l$, then by *(ii)*, there exists $g_1, \ldots, g_t \in A$ such that

$$h_i = \textstyle\sum_{j=1}^{t} g_j f_j,$$

and for all $j \leq t$, $\mathrm{lt}(h_i) \geq_T \mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)$ which implies that for some $j \leq t$,

$$\mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j) = \mathrm{lt}(h_i).$$

Thus, $\mathrm{lt}(h_i) \in \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_t) \rangle$, and this holds for $i = 1, \ldots, t$. Now Equation 2.2 implies

$$h \in \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_t) \rangle,$$

and hence $\mathrm{lt}(\mathcal{I}) \subseteq \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_t) \rangle$. Therefore, F is a Gröbner basis for $\mathcal{I}$ since $\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_t) \rangle \subseteq \mathrm{lt}(\mathcal{I})$ always holds.

(ii⇒iii) Let $f \in \mathcal{I} \setminus \{0\}$, then $f = \sum_{j=1}^{t} g_j f_j$ where $\mathrm{lt}(f) \geq_T \mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)$ for all j. Let

$$\max\{\mathrm{lt}(g_j) \cdot \mathrm{lt}(f_j)\} = T_1 \cdot \mathrm{lt}(f_{s_1}).$$

where $T_1 \in \mathcal{T}$. Then by *(ii)*, $\mathrm{lt}(f) = T_1 \cdot \mathrm{lt}(f_{s_1})$, and there exists $c_1 \in K$ so that if

$$h_1 = f - c_1 T_1 \cdot f_{s_1},$$

h_1 is a rewriting of f with $h_1 \in \mathcal{I}$ and $\mathrm{lt}(h_1) <_T \mathrm{lt}(f)$. Thus $f \xrightarrow{F} h_1$, and if $h_1 \neq 0$, then *(ii)* holds for h_1. It follows that there exists $s_2 \leq t$ and $c_2 \in K$ so that if

$$h_2 = h_1 - c_2 T_2 f_{s_2},$$

h_2 is a rewriting of h_1 with $h_2 \in \mathcal{I}$ and $\mathrm{lt}(h_2) <_T \mathrm{lt}(h_1)$. Therefore, $h_1 \xrightarrow{F} h_2$. We continue this procedure and note that at each step $\mathrm{lt}(h_i) <_T \mathrm{lt}(h_{i-1})$. It follows that there exists k where $h_k = 0$. Hence

$$f \xrightarrow{F} h_1 \xrightarrow{F} h_2 \xrightarrow{F} \cdots \xrightarrow{F} h_{k-1} \xrightarrow{F} h_k = 0.$$

By transitivity of $\xrightarrow{F}$, $f \xrightarrow{F} 0$.

If $f \xrightarrow{F} 0$, then $f \in \mathcal{I}$ since Remark 1 indicates that f will be a linear combination of elements from F.

(iii⇒ii) Pick $f \in \mathcal{I} \setminus \{0\}$. Then $f \xrightarrow{F} 0$ and by Remark 1, there exists $p_j \in F$, $T_j \in \mathcal{T}$, and $c_j \in K$ such that

$$f = \sum_{j=1}^{m} \frac{c_j}{\mathrm{lc}(p_j)} \cdot T_j \cdot p_j,$$

and for all $i \leq m$, $T_i \cdot \mathrm{lt}(p_i) \leq_T \mathrm{lt}(f)$. By collecting terms in the sum with common $p_i \in F$, *(ii)* is obtained. □

Part *(ii)* of Theorem 2.1 serves to link part *(i)* and *(iii)*, as well as to prove another characterization of Gröbner basis to be introduced later.

Before stating the next theorem, it is necessary to fix a grading on A and on A^t, for t a natural number. A is given the natural $\mathbf{Z}^n$-grading by setting

$$A_{(a_1,\ldots,a_n)} = \{cx_1^{a_1}\ldots x_n^{a_n} \mid c \in K\}.$$

Consider the free A-module, A^t, with the following $\mathbf{Z}^n$-grading:

$$A^t_{(a_1,\ldots,a_n)} = \{(c_1T_1,\ldots,c_tT_t) \mid \forall i,\ \deg(T_i) + \deg(f_i) = (a_1,\ldots,a_n)\},$$

where $F = \{f_1, f_2, \ldots, f_t\} \subseteq A$ and the order of F is fixed. With respect to this grading, we say $R = (r_1,\ldots,r_t) \in A^t$ is *homogeneous* of degree $(a_1,\ldots,a_n)$ if for every $i \leq t$, $r_i = c_iT_i$ is a monomial with $c_i \in K$ and $T_i \in \mathcal{T}$, and for every i, $\deg(T_if_i) = (a_1,\ldots,a_n)$ is fixed. When $R \in A^t$ is not homogeneous, we direct our attention to the r_if_i that have maximum degree.

DEFINITION 5 *Let $F = \{f_1, f_2, \ldots, f_t\} \subseteq A \setminus \{0\}$ and $R = (r_1,\ldots,r_t) \in A^t$. The* **(multi)degree** *of R, denoted $deg(R)$, is the degree of r_mf_m, where $lt(r_mf_m) = \max\{lt(r_if_i) \mid i = 1,\ldots,t\}$.*

Although $\deg(R)$ where $R \in A^t$ and $\deg(f)$ where $f \in A$ are both elements of $\mathbf{Z^n}$, the reader will need to distinguish between $\deg(R)$ defined above and $\deg(f)$ defined in Definition 1*(vii)*.

To establish our last equivalence of Gröbner basis, it is necessary to define the following three mappings which are described in Robbiano (p. 37).

DEFINITION 6 *Let $F = \{f_1, f_2, \ldots, f_t\} \subseteq A$, where the order of F is fixed, and $R = (r_1,\ldots,r_t) \in A^t$.*

(i) $\lambda\colon A^t \longrightarrow A$ *where* $\lambda(R) = \sum_{i=1}^t r_if_i$;

(ii) $\mu\colon A^t \longrightarrow A$ *where* $\mu(R) = \sum_{i=1}^t r_i \cdot lm(f_i)$;

(iii) $\mathrm{M}^+\colon A^t \longrightarrow A^t$ *where* $\mathrm{M}^+(R) = \bar{R} = (\bar{r}_1,\ldots,\bar{r}_t)$ *with*

$\bar{r}_i = 0$ *if* $deg(r_if_i) < deg(R)$,

$\bar{r}_i = lm(r_i)$ *if* $deg(r_if_i) = deg(R)$.

It follows from the above definition that λ and μ are both A-module homomorphisms.

REMARK 2 *For any $R \in A^t$, by definition of M^+, $\mathrm{M}^+(R)$ is homogeneous of degree that of R. If R is homogeneous in A^t, $\mathrm{M}^+(R) = R$.*

If R is not homogeneous, we are interested in $H \in A^t$ such that $\mathrm{M}^+(R) = H$.

DEFINITION 7 *Let $R = (r_1, \ldots, r_t) \in A^t$ and $H = (h_1, \ldots, h_t)$ be a homogeneous element of A^t. H* **extends** *to R if $\mathrm{M}^+(R) = H$.*

The following lemma provides tools which will be used to prove our last characterization of Gröbner bases.

LEMMA 1 *Let $F = \{f_1, f_2, \ldots, f_t\} \subseteq A \setminus \{0\}$ be fixed and $R = (r_1, \ldots, r_t) \in A^t$. With respect to the preceding definitions, the following hold:*

(i) *$deg(\lambda(R)) \leq deg(R)$.*

(ii) *If $R \in ker(\lambda)$, then an element of $ker(\mu)$ extends to R.*

(iii) *If $R \notin ker(\lambda)$, then $deg(\lambda(R)) < deg(R)$ iff an element of $ker(\mu)$ extends to R.*

PROOF *(i)* This follows directly from the definitions of λ and (multi)degree.

(ii) It suffices to show that $\mathrm{M}^+(R) \in \ker(\mu)$ for any $R \in \ker(\lambda)$. Pick $R \in \ker(\lambda)$, then

$$\lambda(R) = \textstyle\sum_{i=1}^{t} r_i f_i = 0.$$

which implies that, in the sum the maximal terms, $\bar{r_i} \cdot \mathrm{lm}(f_i)$ where $\bar{r_i} \neq 0$, must cancel. In other words,

$$0 = \sum_{i=1}^{t} \bar{r_i} \mathrm{lm}(f_i) = \mu(\mathrm{M}^+(R)). \tag{2.3}$$

(iii) Pick $R \in A^t \backslash \ker(\lambda)$, suppose $\deg(\lambda(R)) < \deg(R)$. Therefore, by definition of λ and (multi)degree,

$$\mathrm{lt}(\textstyle\sum_{i=1}^{t} r_i f_i) <_T \max\{\mathrm{lm}(r_i f_i)\}.$$

Hence the maximal terms cancel in the sum, and so 2.3 holds. Thus $\mathrm{M}^+(R) \in \ker(\mu)$.

On the other hand, if $\mathrm{M}^+(R) \in \ker(\mu)$, then

$$\mu(\mathrm{M}^+(R)) = \sum_{i=1}^{t} \bar{r}_i \mathrm{lm}(f_i) = 0.$$

This implies

$$\deg\left(\textstyle\sum_{i=1}^{t} r_i f_i\right) < \deg(\max\{r_i f_i\}).$$

And since $\deg(\lambda(R)) = \deg\left(\sum_{i=1}^{t} r_i f_i\right)$ and $\deg(R) = \deg(\max\{r_i f_i\})$, we have the result. □

The following theorem is essential in establishing that there exists an algorithm which transforms an arbitrary generating set of an ideal $\mathcal{I}$ into a Gröbner basis for $\mathcal{I}$.

THEOREM 2.2 *Let $\mathcal{I} = \langle f_1, f_2, \ldots, f_t \rangle$ with $F = \{f_1, f_2, \ldots, f_t\} \subseteq A = K[x_1, \ldots, x_n]$ where K is a field. The following are equivalent:*

(i) *F is a Gröbner basis for $\mathcal{I}$;*

(ii) *every homogeneous element of $\ker(\mu)$ extends to an element of $\ker(\lambda)$.*

PROOF *(i⇒ii)* Let $H = (h_1, \ldots, h_t) \in A^t$ be a nonzero homogeneous element of $\ker(\mu)$. As noted in Remark 2, $\mathrm{M}^+(H) = H$, therefore if $H \in \ker(\lambda)$, then we are done. Assume $0 \neq \lambda(H) = \sum_{i=1}^{t} h_i f_i \in \mathcal{I}$, and F is a Gröbner basis for $\mathcal{I}$, Theorem 2.1*(ii)* yields

$$\lambda(H) = \textstyle\sum_{i=1}^{t} g_i f_i,$$

for some $g_i \in A$ with $\mathrm{lt}(\lambda(H)) = \max\{\mathrm{lt}(g_i) \cdot \mathrm{lt}(f_i)\}$. If $G = (g_1, \ldots, g_t)$, then $\lambda(G) = \lambda(H)$ and $\deg(G) = \deg(\lambda(H))$.

Since $H \notin \ker(\lambda)$, Lemma 1 *(iii)* implies

$$\deg(H) > \deg(\lambda(H)) = \deg(G).$$

Therefore, $\mathrm{M}^+(H - G) = \mathrm{M}^+(H) = H$, and since

$$\sum_{i=1}^{t}(h_i - g_i)f_i = 0,$$

$H - G \in \ker(\lambda)$.

(ii⇒i) Let $f \in \mathcal{I}\backslash\{0\}$, then $f = \sum_{i=1}^{t} g_i f_i$ for some $g_i \in A$. Let $G = (g_1, \ldots, g_t)$. Then $\lambda(G) = f$ and by Lemma 1 *(i)*, $\deg(f) \leq \deg(G)$.

If $\deg(f) = \deg(G)$, then the conclusion of Theorem 2.1 *(ii)* holds. Suppose $\deg(f) < \deg(G)$. Then since $f \neq 0$, $G \notin \ker(\lambda)$, and it follows from Lemma 1 *(iii)* that $\mathrm{M}^+(G) \in \ker(\mu)$. The hypothesis implies that since $\mathrm{M}^+(G)$ is homogeneous there exists $K \in \ker(\lambda)$ such that $\mathrm{M}^+(K) = \mathrm{M}^+(G)$. Let

$$G_1 = G - K = (g_{11}, g_{12}, \ldots, g_{1t}) \in A^t.$$

Then $\deg(G_1) < \deg(G)$ by definition of M^+ and the fact that $\mathrm{M}^+(K) = \mathrm{M}^+(G)$. Futhermore, $f = \lambda(G_1)$ since $K \in \ker(\lambda)$ and λ is a homomorphism.

Repeating this process, if necessary, we obtain a $G_r \in A^t$ so that $\lambda(G_r) = f$ and $\deg(G_r) = \deg(f)$. Therefore, Theorem 2.1 *(ii)* holds, and hence F is a Gröbner basis for $\mathcal{I}$. □

By way of Theorem 2.1 and 2.2, we have established three conditions equivalent to Definition 1 of a Gröbner basis. Although Definition 1 is perhaps the easiest to apply as a test for a Gröbner basis, the equivalent conditions are essential to verify the correctness of the algorithm which computes a Gröbner basis.

2.2 Construction of Gröbner Bases

Much of the same notation and many of the ideas from Section 2.1 are utilized in this section as we develop an efficient procedure for constructing a Gröbner basis. In particular, we use the mappings, λ, μ, and M^+ as defined in Definition 6.

Before presenting the algorithm which computes a Gröbner basis, it is convenient to introduce the following notation used by Robbiano (p. 43).

DEFINITION 8 *Let* $F = \{f_1, \ldots, f_r\} \subseteq A = K[x_1, \ldots, x_n]$, *where* K *is a field. Let* $(e_1, \ldots, e_r)$ *be the canonical basis of* A^r.

(i) $B = \{(i,j) \mid 1 \leq i < j \leq r\}$;

(ii) $L(i,j) = lcm(lt(f_i), lt(f_j))$ *for* $(i,j) \in B$;

(iii) $s(i,j) = \frac{L(i,j)}{lm(f_i)} e_i - \frac{L(i,j)}{lm(f_j)} e_j$.

Notice that s(i,j) is an element of A^r and has zeros everywhere except in the i-th and j-th places, and therefore λ(s(i,j)) is a linear combination of f_i and f_j.

DEFINITION 9 *Let* $F = \{f_1, f_2, \ldots, f_r\} \subseteq A$.

$$S(i,j) \equiv \lambda(s(i,j)) = \frac{L(i,j)}{lm(f_i)} f_i - \frac{L(i,j)}{lm(f_j)} f_j$$

is called the **S-polynomial** *of* f_i *and* f_j.

The example below illustrates the function of the S-polynomial in the construction of a Gröbner basis. Assume the monomials of A are ordered with respect to the pure lexicographical ordering.

EXAMPLE 2.5 Let $F = \{f_1, f_2\}$ where $f_1 = x^2y + 2x$ and $f_2 = y^2 + 3x^3$. The S-polynomial of f_1 and f_2,

$$\mathrm{S}(1,2) = 2xy - 3x^5.$$

Observe that the F of example 2.5 is *not* a Gröbner basis for $\mathcal{I} = \langle f_1, f_2 \rangle$ since $\mathrm{lt}(\mathrm{S}(1,2)) \in \mathrm{lt}(\mathcal{I})$, but $\mathrm{lt}(\mathrm{S}(1,2)) = xy \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle$. In fact, to build a Gröbner basis from F, it is necessary to adjoin to F a polynomial, f_3, from $\mathcal{I}$ which will guarantee $\mathrm{lt}(\mathrm{S}(1,2)) \in \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \mathrm{lt}(f_3) \rangle$.

The S-polynomial is fundamental to the decision process involved in transforming a given set $F = \{f_1, f_2, \ldots, f_t\}$ into a Gröbner basis for $\mathcal{I} = \langle f_1, f_2, \ldots, f_t \rangle$. To achieve a Gröbner basis for $\mathcal{I}$, we will adjoin to F a reduced form of each S-polynomial that cannot be rewritten to zero.

The correctness of the algorithmic characterization for a Gröbner basis essentially depends on the next lemma.

LEMMA 2 *Let $F = \{f_1, f_2, \ldots, f_r\} \subseteq A \setminus \{0\}$. With respect to the preceding definitions, the following hold:*

(i) *$s(i,j)$ is homogeneous and $deg(s(i,j)) = deg(L(i,j))$;*

(ii) *$S(B) = \{s(i,j) \mid (i,j) \in B\}$ is a basis of $ker(\mu)$;*

(iii) *if $S(i,j) \xrightarrow{F} 0$, then $s(i,j)$ extends to an element of $ker(\lambda)$;*

(iv) *if $L(i,j) = lt(f_i) \cdot lt(f_j)$, then $s(i,j)$ extends to an element of $ker(\lambda)$.*

PROOF *(i)* Let $(i,j) \in B$. Note that

$$\deg\left(\frac{\mathrm{L}(i,j)}{\mathrm{lm}(f_i)} f_i\right) = \deg\left(\frac{\mathrm{L}(i,j)}{\mathrm{lm}(f_j)} f_j\right) = \deg(\mathrm{L}(i,j)).$$

Therefore,

$$\mathrm{s}(i,j) = \left(0, \ldots, \frac{\mathrm{L}(i,j)}{\mathrm{lm}(f_i)}, \ldots, 0, \ldots, -\frac{\mathrm{L}(i,j)}{\mathrm{lm}(f_j)}, \ldots, 0\right)$$

is homogeneous with degree that of $\mathrm{L}(i,j)$.

(ii) By definition of a graded ring, it suffices to show that $\mathrm{S}(B)$ is a basis for the homogeneous elements of $\ker(\mu)$.

Without loss of generality, assume $\mathrm{lc}(f_i) = 1$ for all $i \leq r$. Let $S = (s_1, \ldots, s_r)$ be a homogeneous element of $\ker(\mu)$. According to the $\mathbf{Z}^n$-grading fixed on A^r, for

each $i \leq r$, there exists $c_i \in K$ and $T_i \in \mathcal{T}$ so that $s_i = c_i T_i$, and $\deg(T_i \cdot \mathrm{lt}(f_i))$ is the same for each i. In other words,

$$T_1 \cdot \mathrm{lt}(f_1) = \cdots = T_r \cdot \mathrm{lt}(f_r).$$

Therefore, there exists $T \in \mathcal{T}$ with

$$T_1 = T \cdot \frac{\mathrm{L}(1,2)}{\mathrm{lt}(f_1)} \quad \text{and} \quad \mathrm{T}_2 = \mathrm{T} \cdot \frac{\mathrm{L}(1,2)}{\mathrm{lt}(f_2)}.$$

Let $s^\star = -c_1 T_2$, then

$$(s_1, s^\star, 0, \ldots, 0) = c_1 T \cdot \mathrm{s}(1,2),$$

and $\bar{S} = S - (s_1, s^\star, 0, \ldots, 0)$ is a homogeneous element of $\ker(\mu)$ with first component zero. Repeat this argument until all but two entries are zero. Note that the ith $s^\star$ equals $-(c_i + c_{i-1} + \cdots + c_1) \cdot T_{i+1}$.

Suppose $\bar{s}_i$ and $\bar{s}_j$ are the only two nonzero entries of $\bar{S}$. Since $\bar{S} \in \ker(\mu)$, then

$$\bar{s}_i \cdot \mathrm{lm}(f_i) = -\bar{s}_j \cdot \mathrm{lm}(f_j).$$

Therefore, there exists $h \in A$ such that

$$h \cdot \mathrm{L}(i,j) = \bar{s}_i \cdot \mathrm{lm}(f_i) = -\bar{s}_j \cdot \mathrm{lm}(f_j).$$

It follows that $\bar{S} = h \cdot \mathrm{s}(i,j)$, and hence S is a linear combination of elements from $\mathrm{S}(B)$.

(iii) Assume $\mathrm{S}(i,j) \xrightarrow{F} 0$. From Remark 1 of Section 2.1, it follows that there exists $g_1, \ldots, g_r \in A$ such that

$$\mathrm{S}(i,j) = \textstyle\sum_{k=1}^{r} g_k f_k$$

where $\deg(\mathrm{S}(i,j)) = \max\{\deg g_k f_k\}$. Also note that

$$\mathrm{M}^+(\mathrm{s}(i,j)) = \mathrm{s}(i,j) \in \ker(\mu).$$

So if $\mathrm{s}(i,j) \in \ker(\mu)$, then we are done. Otherwise, by Lemma 1 *(iii)*,

$$\deg(\mathrm{s}(i,j)) > \deg(\mathrm{S}(i,j)).$$

Let $R = \mathrm{s}(i,j) - \sum_{k=1}^{r} g_k e_k$, then $R \in \ker(\lambda)$ and $\mathrm{M}^+(R) = \mathrm{s}(i,j)$.

(iv) Suppose $\mathrm{L}(i,j) = \mathrm{lt}(f_i) \cdot \mathrm{lt}(f_j)$. Then

$$\mathrm{s}(i,j) = \frac{\mathrm{lt}(f_j)}{\mathrm{lc}(f_i)} e_i - \frac{\mathrm{lt}(f_i)}{\mathrm{lc}(f_j)} e_j,$$

and if

$$R = \frac{f_j}{\mathrm{lc}(f_i f_j)} e_i - \frac{f_i}{\mathrm{lc}(f_i f_j)} e_j,$$

then $R \in \ker(\lambda)$ and $\mathrm{M}^+(R) = \mathrm{s}(i,j)$. □

We are now ready to describe the algorithm presented in Robbiano (p. 44), known as Buchberger's algorithm, which computes a Gröbner basis for ideals in $A = K[x_1, \ldots, x_n]$, where K is a field. Assume a total ordering has been fixed on the terms of A.

ALGORITHM 2.1 (BUCHBERGER)

Input: $f_1, f_2, \ldots, f_r \in A \setminus \{0\}$.

Output: A Gröbner basis of $\mathcal{I} = \langle f_1, f_2, \ldots, f_r \rangle$.

Begin: LET $F = \{f_1, f_2, \ldots, f_r\}$; $u = r$; $B = \{(i,j) \mid 1 \le i < j \le u\}$.

WHILE $B \neq \emptyset$ DO

CHOOSE $(i,j) \in B$

$B = B \setminus \{(i,j)\}$

IF $L(i,j) \neq lt(f_i) \cdot lt(f_j)$ THEN

$f = S(i,j)$

WHILE $f \neq 0$ *and* $lt(f) \in lt(F)$ DO

CHOOSE T *and* s *such that* $lt(f) = T \cdot lt(f_s)$

$f = f - \dfrac{lc(f)}{lc(f_s)} \cdot T \cdot f_s$

IF $f \neq 0$ THEN

$u = u + 1$

$f_u = f$

$F = F \cup \{f_u\}$

$$B = B \cup \{(i,u) \mid 1 \leq i < u\}.$$

The final theorem of this section verifies the correctness of Buchberger's algorithm.

THEOREM 2.3 *Given* $F = \{f_1, f_2, \ldots, f_r\} \subseteq A \setminus \{0\}$ *where* $A = K[x_1, \ldots, x_n]$. *Then Buchberger's algorithm computes a Gröbner basis for* $\mathcal{I} = \langle f_1, f_2, \ldots, f_r \rangle$.

PROOF Each time the S-polynomial does not reduce to zero, we adjoin to F a new element from $\mathcal{I}$ in which the leading term does not belong to the preceding $\mathrm{lt}(F)$. Say f_{s_i} is the i-th element added to F and let $H_1 = \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_r), \mathrm{lt}(f_{s_1}) \rangle$ and $H_i = \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_r), \ldots, \mathrm{lt}(f_{s_i}) \rangle$. If the algorithm does not terminate, then

$$\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_r) \rangle = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_i \subseteq \cdots$$

does not stabilize. But this contradicts that A is Noetherian. Hence the algorithm does terminate.

Assume $F = \{f_1, \ldots, f_t\}$ is the output and $B = \{(i,j) \mid 1 \leq i < j \leq t\}$. Pick $(i,j) \in B$. Note if $\mathrm{L}(i,j) = \mathrm{lt}(f_i) \cdot \mathrm{lt}(f_j)$, then by Lemma 2*(iv)*, $\mathrm{s}(i,j)$ extends to an element of $\ker(\lambda)$. Furthermore, if $\mathrm{L}(i,j) \neq \mathrm{lt}(f_i) \cdot \mathrm{lt}(f_j)$, then, since the algorithm terminates, $\mathrm{S}(i,j) \xrightarrow{F} 0$ which via Lemma 2*(iii)* implies $\mathrm{s}(i,j)$ extends to an element of $\ker(\lambda)$. Therefore, by Lemma 2*(i)* and 2*(ii)*,

$$\mathrm{S}(B) = \{\mathrm{s}(i,j) \mid (i,j) \in B\}$$

is a homogeneous basis of $\ker(\mu)$ that extends to elements of $\ker(\lambda)$. We will now show that every homogeneous element of $\ker(\mu)$ extends and use Theorem 2.2.

Rename the elements of $\mathrm{S}(B)$ so $\mathrm{S}(B) = \{B_1, \ldots, B_s\}$, where for each i, $B_i = \mathrm{s}(i',j') = (b_{i1}, \ldots, b_{it})$. Let $H = (h_1, \ldots, h_t)$ be a nonzero homogeneous element of $\ker(\mu)$. Thus $H = \sum_{i=1}^{s} m_i B_i$ where m_i are monomials of A such that for each i, where $m_i \neq 0$,

$$\deg(m_i) + \deg(B_i) = \deg(H).$$

For every $i = 1, \ldots, s$, since B_i extends, we can pick $S_i \in \ker(\lambda)$ so that $\mathrm{M}^+(S_i) = B_i$. Then by definition of M^+, for every $j = 1, \ldots, t$, either $b_{ij} = 0$ or $b_{ij} = \mathrm{lm}(s_{ij})$, where s_{ij} is the j-th component of S_i. Let $L = \sum_{i=1}^{s} m_i S_i$. Note that $L \in \ker(\lambda)$.

Since

$$\deg(B_i) = \deg(\mathrm{M}^+(B_i)) = \deg(S_i),$$

then for all i, $\deg(m_i) + \deg(S_i) = \deg(H)$. Consider $\mathrm{M}^+(L) = \bar{L} = (\bar{l}_1, \ldots, \bar{l}_t)$. We wish to show that $\mathrm{M}^+(L) = H$.

Fix j and let $U = \{k \mid \deg(s_{kj}) = \deg(S_k)\}$. Now $l_j = \sum_{i=1}^{s} m_i s_{ij}$ and $\bar{l}_j = 0$ or $\bar{l}_j = \mathrm{lm}(\sum_{i=1}^{s} m_i s_{ij})$. If $\bar{l}_j = 0$, then

$$\deg(f_j \cdot \mathrm{lm}(\textstyle\sum_{i=1}^{s} m_i s_{ij})) = \deg(f_j l_j) < \deg(L) = \deg(m_n) + \deg(S_n)$$

for every $n = 1, \ldots, s$. Then $\sum_{i \in U} m_i \mathrm{lm}(s_{ij}) = 0$ and for every $i \notin U$, $b_{ij} = 0$. Hence

$$h_j = \sum_{i=1}^{s} m_i b_{ij} = 0 = \bar{l}_j.$$

If $\bar{l}_j = \mathrm{lm}(\sum_{i=1}^{s} m_i s_{ij})$, then $\deg(l_j f_j) = \deg(L)$. Thus

$$\bar{l}_j = \sum_{i \in U} m_i \cdot \mathrm{lm}(s_{ij}) = \sum_{i \in U} m_i b_{ij}.$$

Since for each $i \notin U$, $b_{ij} = 0$, $\bar{l}_j = \sum_{i=1}^{s} m_i b_{ij} = h_j$. So $\mathrm{M}^+(L) = H$ and every homogeneous element of $\ker(\mu)$ extends to an element of $\ker(\lambda)$. It follows from Theorem 2.2, that F is a Gröbner basis for $\mathcal{I}$. □

The following example outlines an application of Algorithm 2.1.

EXAMPLE 2.6 Let $F = \{f_1, f_2, f_3\}$ where

$$f_1 = z^3 + xy, \quad f_2 = xz^2 - y, \quad f_3 = y + x^2.$$

The pure lexicographical ordering of terms is used with $x < y < z$. The nonzero reductions of the S-polynomials of f_i and f_j where $\mathrm{L}(i,j) \neq \mathrm{lt}(f_i) \cdot \mathrm{lt}(f_j)$ are shown below:

$$\mathrm{S}(1,2) = yz + x^2 y,$$

$$S(1,2) \xrightarrow{F} f_4 = S(1,2) - zf_3 = -x^2z + x^2y.$$

Next $F = \{f_1, f_2, f_3, f_4\}$ and the next S-polynomial is:

$$S(2,4) = x^2yz - xy.$$

Note that

$$S(2,4) \xrightarrow{F} f_5 = S(2,4) - x^2zf_3 - x^2f_4 + x^4f_3 + xf_3 = x^6 + x^3.$$

Now, $F = \{f_1, \ldots, f_5\}$ is a Gröbner basis for $\mathcal{I} = \langle f_1, f_2, f_3 \rangle$ since further S-polynomials have leading terms in $\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2), \mathrm{lt}(f_3) \rangle$.

Theorem 2.3 establishes that any finite generating set for an ideal $\mathcal{I}$ can be algorithmically transformed into a Gröbner basis for $\mathcal{I}$. Although such a basis is not unique, it can be written in a unique form.

DEFINITION 10 *Let $F = \{f_1, f_2, \ldots, f_t\} \subseteq A = K[x_1, \ldots, x_n]$ be a Gröbner basis for $\mathcal{I} = \langle f_1, f_2, \ldots, f_t \rangle$. F is a* **reduced Gröbner basis** *for $\mathcal{I}$ if for all $j, i \leq t$, no term of f_i is a multiple of $lt(f_j)$ for each $j \neq i$.*

THEOREM 2.4 *Suppose a total ordering on the monomials of A has been fixed. For every ideal $\mathcal{I}$ of A there exists a unique (up to units) reduced Gröbner basis of $\mathcal{I}$.*

The reader is referred to Robbiano (p. 42) for the proof of this theorem.

Any Gröbner basis, $F = \{f_1, f_2, \ldots, f_t\}$ of $\mathcal{I} = \langle f_1, f_2, \ldots, f_t \rangle$, can be transformed into a reduced Gröbner basis of $\mathcal{I}$ by reducing each f_i via F and dividing each f_i by $\mathrm{lc}(f_i)$. The reduced Gröbner basis for $\mathcal{I} = \langle f_1, f_2, f_3 \rangle$ of Example 2.6 is

$$F = \{z^3 - x^3, xz^2 + x^2, y + x^2, x^2z + x^4, x^6 + x^3\}.$$

There are variations of Algorithm 2.1, as in Buchberger (1985, pp. 196-197), that include subroutines designed to speed up computations and to produce the

reduced Gröbner basis of $\mathcal{I}$. Computer programs, such as MAPLE, are available which utilize these algorithms thus allowing mathematicians to concentrate on the interesting applications of Gröbner bases, not their tedious construction.

The remainder of this paper focuses on the application of Gröbner bases to primary decomposition of ideals in $K[x, y]$.

Chapter 3

Primary Decomposition of Ideals in $K[x, y]$ via Gröbner Basis

In this chapter, the study of primary decomposition is restricted to ideals in the polynomial ring $K[x, y]$, where K is a field. It will be shown that a primary decomposition of an ideal $\mathcal{I}$ of $K[x, y]$ can be algorithmically computed given a Gröbner basis of $\mathcal{I}$.

Throughout the chapter, the reader should assume that the monomials of $K[x, y]$ are ordered with respect to the pure lexicographical ordering:

$$1 < x < x^2 < \cdots < y < xy < x^2y < \cdots < y^2 < xy^2 < \cdots.$$

3.1 Structure of Gröbner Basis

The elements of $K[x, y]$ will be considered as polynomials in y with coefficients in $K[x]$. The definition below fixes notation relating to this perspective.

DEFINITION 1 *Let $f \in K[x, y] \setminus \{0\}$, where K is a field.*

(i) *content(f) $\in K[x]$ denotes the* **content** *of f which is a polynomial in $K[x]$ of greatest degree which divides f.*

(ii) *primpart*$(f) \in K[x,y]$ *denotes the* primary part *of* f *which is* $\dfrac{f}{content(f)}$.

(iii) *coef*$(f, y^n) \in K[x]$ *is the polynomial in* $K[x]$ *which is the* **coefficient** *of the term* y^n *of* f.

(iv) $d(f) \in \mathbf{N}$ *is the* **degree of** y *in the leading monomial of* f *with respect to the pure lexicographical ordering.*

(v) $LC(f) = coef(f, y^{d(f)})$ *denotes the* **leading coefficient** *of* f *and is the polynomial in* $K[x]$ *which is the coefficient of the term* $y^{d(f)}$ *of* f.

Some of the notation from Chapter 2 relating to Gröbner bases will also be used such as $\mathrm{lm}(f)$, $\deg(f)$, $\mathrm{lt}(\mathcal{I})$, etc. It is important to note that $\mathrm{LC}(f)$ is not necessarily the same as $\mathrm{lc}(f)$ of Definition 1 in Chapter 2. Furthermore, $\mathrm{d}(f)$ differs from $\deg(f)$.

Before presenting the first theorem, we introduce a notion slightly weaker than that of a reduced Gröbner basis.

DEFINITION 2 *Let* $F = \{f_1, f_2, \ldots, f_t\} \in A = K[x_1, \ldots, x_n]$ *be a Gröbner basis for* $\mathcal{I} = \langle f_1, f_2, \ldots, f_t \rangle$. F *is a* **minimal Gröbner basis** *for* $\mathcal{I}$ *if for every* $j, i \leq t$, $lt(f_i)$ *does not divide* $lt(f_j)$ *for each* $j \neq i$.

In general, a minimal Gröbner basis, unlike a reduced Gröbner basis, is not unique. Note that a reduced Gröbner basis is a minimal Gröbner basis. The following theorem presented in Lazard (1985, p. 262) introduces a general structure of a minimal Gröbner basis for ideals of $K[x,y]$.

THEOREM 3.1 *Let* $\mathcal{I} = \langle f_0, \ldots, f_k \rangle$ *be an ideal in* $K[x,y]$ *where* $F = \{f_0, \ldots, f_k\} \subseteq K[x,y]$ *is a minimal Gröbner basis for* $\mathcal{I}$ *ordered by increasing leading monomials. Then for each* $i = 0, 1, \ldots, k$,

$$f_i = PH_iG_{i+1} \cdots G_{k+1}$$

where

$$P = primpart(f_0) \quad and \quad G_{k+1} = content(f_k),$$

$$H_i \in K[x,y] \quad is\ monic\ in \quad y,$$

and for $i = 0, \ldots, k-1$,

$$G_{i+1} = \frac{LC(f_i)}{LC(f_{i+1})} \in K[x].$$

Theorem 3.1 is proved by means of six lemmas which have the same hypothesis as the theorem.

LEMMA 1 *For each* $i = 1, \ldots, k$, $d(f_{i-1}) < d(f_i)$.

PROOF Since F is ordered by increasing leading monomials, $\mathrm{d}(f_{i-1}) \leq \mathrm{d}(f_i)$. Now

$$\mathrm{lm}(f_{i-1}) = c_{i-1}x^l y^{\mathrm{d}(f_i)} \quad \text{and} \quad \mathrm{lm}(f_i) = c_i x^j y^{\mathrm{d}(f_i)}$$

for some $c_{i-1}, c_i \in K$ and $j, l \in \mathbf{N}$. Since F is a minimal Gröbner basis, $l > j$ and $\mathrm{d}(f_{i-1}) < \mathrm{d}(f_i)$. □

LEMMA 2 *For each* $i = 1, \ldots, k$, $LC(f_i)$ *divides* $LC(f_{i-1})$.

PROOF Choose $i \in \{1, \ldots, k\}$. By Lemma 1, $\mathrm{d}(f_i) - \mathrm{d}(f_{i-1}) > 0$. Clearly, $y^{\mathrm{d}(f_i)-\mathrm{d}(f_{i-1})} f_{i-1}$ and f_i are polynomials in $\mathcal{I}$ each with degree in y equal to $\mathrm{d}(f_i)$. Let $g_i = \mathrm{LC}(f_i)$ and set $d = \gcd(g_{i-1}, g_i)$. Then there exists $a, b \in K[x]$ such that $d = ag_{i-1} + bg_i$. Consider

$$h = ay^{\mathrm{d}(f_i)-\mathrm{d}(f_{i-1})} f_{i-1} + bf_i \in \mathcal{I}.$$

Then there exists $m_{i-1}, m_i \in K[x,y]$ with $\mathrm{d}(m_{i-1}), \mathrm{d}(m_i) < \mathrm{d}(f_i)$ such that

$$h = dy^{\mathrm{d}(f_i)} + am_{i-1} + bm_i.$$

Since $h \in \mathcal{I}$ and F is a Gröbner basis for $\mathcal{I}$, $\mathrm{lm}(h) \in \mathrm{lt}(F)$. Therefore, there exists monomials $q_i \in K[x,y]$ where

$$\mathrm{lt}(h) = \sum_{j=0}^{k} q_j \cdot \mathrm{lt}(f_j).$$

In fact, there exists $j \leq i$,

$$\mathrm{lt}(h) = \mathrm{lt}(dy^{\mathrm{d}(f_i)}) = \mathrm{lt}(q_j) \cdot \mathrm{lt}(f_j) = \mathrm{lt}(q_j)y^{\mathrm{d}(f_j)} \cdot \mathrm{lt}(g_j).$$

Therefore,

$$\deg(g_i) \geq \deg(d) \geq \deg(g_j) \geq \deg(g_i)$$

which implies $\deg(d) = \deg(g_i)$, the last inequality following from the proof of Lemma 1. Hence d and g_i differ only by a constant factor. Thus g_i divides g_{i-1}. □

LEMMA 3 *If* $G_{i+1} = \dfrac{LC(f_i)}{LC(f_{i+1})}$, *then* $G_{i+1}f_{i+1} \in \langle f_i, f_{i-1}, \ldots, f_0 \rangle$ *for each* $i = 0, \ldots, k-1$.

PROOF Pick $i \in \{0, \ldots, k\}$. It follows from Lemma 2 that $G_{i+1} = \dfrac{\mathrm{LC}(f_i)}{\mathrm{LC}(f_{i+1})} \in K[x]$. Therefore,

$$h = G_{i+1}f_{i+1} - y^{\mathrm{d}(f_{i+1})-\mathrm{d}(f_i)}f_i \tag{3.1}$$

is an element of $\mathcal{I}$. Since F is a Gröbner basis for $\mathcal{I}$, Theorem 2.1 implies that $h \xrightarrow{F} 0$. Hence, by Remark 1 of Chapter 2,

$$0 = h - \sum_{j=0}^{t} \frac{c_j}{\mathrm{lc}(f_j)} \cdot T_j \cdot f_j \tag{3.2}$$

where for each j, $c_j \in K$, $f_j \in F$, $T_j \in K[x,y]$, and $\max\{\mathrm{lt}(T_jf_j)\} = \mathrm{lt}(h)$. By definition of h,

$$\mathrm{lt}(h) < y^{\mathrm{d}(f_{i+1})} \leq \mathrm{lt}(f_{i+1}).$$

Therefore, for every $j > i$, $c_j = 0$ since F is ordered by leading monomials. Now Equation 3.1 and 3.2 imply

$$G_{i+1}f_{i+1} = y^{\mathrm{d}(f_{i+1})-\mathrm{d}(f_i)}f_i + \sum_{j=0}^{i} \frac{c_j}{\mathrm{lc}(f_j)} \cdot T_j \cdot f_j$$

Therefore, $G_{i+1}f_{i+1} \in \langle f_i, \ldots f_0 \rangle$. □

LEMMA 4 *For each* $i = 0, \ldots, k$, *primpart*(f_0) *divides* f_i.

PROOF Let $P = \text{primpart}(f_0)$. Clearly P divides f_0. Assume that P divides f_j for every $j \leq n < k$. Then for each $j \leq n$, $f_j = h_j P$ for some $h_j \in K[x, y]$. By Lemma 3, there exists $k_j, \ldots, k_0 \in K[x, y]$ such that

$$G_{j+1} f_{j+1} = k_j f_j + k_{j-1} f_{j-1} + \cdots + k_0 f_0.$$

It follows from the induction hypothesis that

$$G_{j+1} f_{j+1} = P(k_j h_j + \cdots + k_0 h_0).$$

Therefore, P divides $G_{j+1} f_{j+1}$. Since P is primitive in $K[x, y]$ and $G_{j+1} \in K[x]$, then Proposition 1 of Chapter 1 yields P divides f_{j+1}. □

LEMMA 5 *If* $\gcd\{f_i\} = 1$, *then for every* $i = 1, \ldots, k$, $LC(f_i)$ *divides* f_i.

PROOF If $\gcd\{f_i\} = 1$, then $P = \text{primpart}(f_0) = 1$ follows from Lemma 4. Therefore, $f_0 \in K[x]$ and by definition, $\text{LC}(f_0) = f_0$. Assume $\text{LC}(f_j)$ divides f_j for every $j \leq n < k$. Then Lemma 2 implies that $\text{LC}(f_j)$ divides f_i for every $i \leq j$. Thus there exists $h_i \in K[x, y]$ so that $f_i = h_i \cdot \text{LC}(f_j)$. Then Lemma 3 yields

$$G_{j+1} f_{j+1} = k_j f_j + \cdots + k_0 f_0 = \text{LC}(f_j) \cdot (k_j h_j + \cdots + k_0 h_0)$$

for some $k_0, \ldots, k_j \in K[x, y]$. In other words,

$$\frac{\text{LC}(f_j)}{\text{LC}(f_{j+1})} f_{j+1} = \text{LC}(f_j) \cdot l$$

where $l \in K[x, y]$. Therefore, $\text{LC}(f_{j+1})$ divides f_{j+1} for each $j < k$. □

LEMMA 6 *If* $\gcd\{f_i\} = 1$, *then* $LC(f_k) = 1$.

PROOF Since for each $j = 0, \ldots, k-1$, $\text{LC}(f_{j+1})$ divides $\text{LC}(f_j)$ and $\text{LC}(f_j)$ divides f_j, then $\text{LC}(f_k)$ divides f_j for all $j \leq k$. Therefore, $\gcd\{f_i\} = 1$ implies $\text{LC}(f_k) = 1$. □

Proof of Theorem 3.1 It suffices to prove that the theorem holds for $\gcd\{f_i\} = 1$. To see this suppose the theorem holds when $\gcd\{f_i\} = 1$, and consider the case when $\gcd\{f_i\} \neq 1$. Then there exists $D \in K[x,y]$ so that for each $i = 1,\ldots,k$,

$$f_i = DF_i \quad \text{and} \quad \gcd(F_0,\ldots,F_k) = 1.$$

Note $\{F_0,\ldots,F_k\}$ is a minimal Gröbner basis for $J = \langle F_0,\ldots,F_k\rangle$ and the theorem holds for $\{F_0,\ldots,F_k\}$. Now $F_0 = PH_0G_1\cdots G_{k+1}$, and so $P = \text{primpart}(F_0)$ implies $H_0 \mid \text{content}(F_0) \in K[x]$, and since H_0 is monic in y, $H_0 = 1$. Furthermore, $P = 1$ and $G_{k+1} = 1$ follows from $\gcd\{F_i\} = 1$ and the fact that for all $i = 0,\ldots,k$,

$$F_i = PH_iG_{i+1}\cdots G_{k+1},$$

where G_i and H_i are defined as in Theorem 3.1. Note for each $i = 1,\ldots,k$,

$$f_i = DH_iG_{i+1}\cdots G_k.$$

In particular, $f_0 = DG_1\cdots G_k$ where $G_1,\ldots,G_k \in K[x]$, which implies that $D = pd$ where $p = \text{primpart}(f_0)$ and $d \in K[x]$. Since $f_k = DH_k = pdH_k$ where H_k is monic in y, $d = \text{content}(f_k)$, and hence $d = G_{k+1}$ for $\{f_i\}$. Therefore, for each $i = 0,1,\ldots,k$,

$$f_i = pH_iG_{i+1}\cdots G_{k+1}$$

where each H_i is monic in y, and for every $i = 0,\ldots,k-1$,

$$\frac{\text{LC}(f_i)}{\text{LC}(f_{i+1})} = \frac{\text{LC}(D)\cdot\text{LC}(F_i)}{\text{LC}(D)\cdot\text{LC}(F_{i+1})} = G_{i+1},$$

and so the theorem holds for $\{f_i\}$.

Now we can assume $\gcd\{f_i\} = 1$, and let $P = \text{primpart}(f_0)$, $G_{k+1} = \text{content}(f_k)$, and, for each $i = 0,\ldots,k$, $H_i = \dfrac{f_i}{\text{LC}(f_i)}$. Then

$$P = 1 = G_{k+1}$$

follows from Lemmas 4 and 6. Furthermore, by Lemma 5, $H_i \in K[x,y]$ is monic in y. Now for each $i \leq k$,

$$f_i = H_i\cdot\text{LC}(f_i) = H_i\cdot\frac{\text{LC}(f_i)}{\text{LC}(f_{i+1})}\cdot\frac{\text{LC}(f_{i+1})}{\text{LC}(f_{i+2})}\cdots\frac{\text{LC}(f_{k-2})}{\text{LC}(f_{k-1})}\cdot\frac{\text{LC}(f_{k-1})}{\text{LC}(f_k)}.$$

Then by canceling common factors and noting that $\mathrm{LC}(f_k) = 1$, by Lemma 6, we obtain

$$f_i = PH_iG_{i+1}\cdots G_{k+1}$$

where for every $i = 0, \ldots, k-1$, $G_{i+1} = \dfrac{\mathrm{LC}(f_i)}{\mathrm{LC}(f_{i+1})} \in K[x]$ by Lemma 2. □

The example below illustrates the structure of a minimal Gröbner basis as described in Theorem 3.1. The reader can assume that $K = \mathbf{R}$, the real numbers.

EXAMPLE 3.1 Let $F = \{f_0, f_1, f_2, f_3\}$ where

$$f_0 = x^7, \quad f_1 = y^2x^5 - yx^6, \quad f_2 = y^4x - y^3x^3, \quad f_3 = y^6 - y^5.$$

Clearly, $1 = G_4 = \mathrm{content}(f_3) = P = \mathrm{primpart}(f_0)$, and $G_{i+1} = \dfrac{\mathrm{LC}(f_i)}{\mathrm{LC}(f_{i+1})}$ yields

$$G_1 = x^2, \quad G_2 = x^4, \quad G_3 = x.$$

Consequently,

$$H_0 = 1, \quad H_1 = y^2 - yx, \quad H_2 = y^4 - y^3x^2, \quad H_3 = y^6 - y^5.$$

3.2 Computation of Primary Components

Theorem 3.1 provides the structure of a minimal Gröbner basis of an ideal in $K[x, y]$ that is essential for Lazard's algorithm (1985, p. 262) which computes the primary components of the ideal. The algorithm is restricted to zero dimensional ideals, i.e. where the minimal primes over such ideals are maximal ideals. However, one dimensional ideals can be treated after removing the greatest common factor of the Gröbner basis, and this decomposition will be discussed at the end of this section.

The application of the algorithm depends on the maximal ideals that contain the ideal in question. These maximal ideals will be computed in Theorem 3.2, the proof of which depends on the following lemma.

LEMMA 7 *Let* $\mathcal{I} = \langle f_0, \ldots, f_k \rangle$ *where* $F = \{f_0, \ldots, f_k\} \subseteq K[x, y]$ *is a minimal Gröbner basis for* $\mathcal{I}$. *Let* F *be ordered by leading monomials and* $\gcd\{f_i\} = 1$. *If* G_j *and* H_j *are defined as in Theorem 3.1, then for every* $j = 1, \ldots, k$, $\mathcal{I} \subseteq \langle H_j, G_j \rangle$.

PROOF Fix $j \in \{1, \ldots, k\}$ and choose $i \in \{0, \ldots, k\}$. By Theorem 3.1, $f_i = PH_iG_{i+1} \cdots G_{k+1}$. Thus if $i \leq j$, then $f_i \in \langle H_j, G_j \rangle$. Now if $i > j$, it suffices to prove that $H_i \in \langle H_j, G_j \rangle$. Using induction on n where $i = j + n$, consider $n = 1$. Since $H_{j+1} = \frac{f_{j+1}}{\mathrm{LC}(f_{j+1})}$ and $G_{j+1} = \frac{\mathrm{LC}(f_j)}{\mathrm{LC}(f_{j+1})}$,

$$G_{j+1}f_{j+1} = \mathrm{LC}(f_j) \cdot H_{j+1}.$$

Then as a result of Lemma 3,

$$\mathrm{LC}(f_j) \cdot H_{j+1} = k_j f_j + \cdots + k_0 f_0$$

where $k_0, \ldots, k_j \in K[x, y]$. Then dividing by $\mathrm{LC}(f_j)$ and using the structure of F,

$$H_{j+1} = k_j H_j + k_{j-1} H_{j-1} G_j + k_{j-2} H_{j-2} G_{j-1} G_j + \cdots + k_1 H_1 G_2 \cdots G_j + k_0 H_0 G_1 \cdots G_j.$$

Therefore, for every $m \leq j$,

$$H_{j+1} \in \langle H_j, H_{j-1}, \ldots, H_{m+1}, H_m, G_m \rangle.$$

In particular, $H_{j+1} \in \langle H_j, G_j \rangle$. Now suppose for each $l < n$, $H_{j+l} \in \langle H_j, G_j \rangle$ and consider H_{j+n}. Note that

$$H_{j+n} \in \langle H_{j+n-1}, H_{j+n-2}, \ldots, H_{j+1}, H_j, G_j \rangle,$$

and, by induction hypothesis,

$$H_{j+n-1}, H_{j+n-2}, \ldots, H_{j+1} \in \langle H_j, G_j \rangle.$$

Hence, $H_{j+n} \in \langle H_j, G_j \rangle$ for any $n \in \mathbf{N}$. In other words,

$$H_i \in \langle H_j, G_j \rangle \tag{3.3}$$

for every $i \geq j$. Therefore, for each i and j, $f_i \in \langle H_j, G_j \rangle$. $\square$

The theorem below provides a characterzation of the maximal ideals containing $\mathcal{I} = \langle f_0, \ldots, f_k \rangle$. It is these maximal ideals which, along with $\{f_0, \ldots, f_k\}$, will be the input for the computation of the primary components of $\mathcal{I}$.

THEOREM 3.2 *Suppose* $F = \{f_0, \ldots, f_k\} \subseteq K[x, y]$ *is structured as in Theorem 3.1 and* $\gcd\{f_i\} = 1$. *Then the following conditions hold:*

(i) *A maximal ideal contains all the* f_i*'s if and only if it contains at least one pair* G_i, H_i.

(ii) *A maximal ideal containing* F *is generated by an irreducible factor* $u(x)$ *of* G_i *in* $K[x]$ *and an irreducible factor* $v(x, y)$ *of* $H_i \bmod u(x)$.

PROOF *(i)* Suppose $\mathcal{M}$ is a maximal ideal in $K[x, y]$ such that $F \subseteq \mathcal{M}$. In particular,

$$f_0 = G_1 \cdots G_{k+1} \in \mathcal{M}$$

which implies that there exists $j \leq k+1$ such that $G_j \in \mathcal{M}$. Say l is greatest such $G_l \in \mathcal{M}$. Then $f_l = PH_lG_{l+1} \cdots G_{k+1}$ implies $H_l \in \mathcal{M}$. Conversely, if $G_l, H_l \in \mathcal{M}$, then it follows from Lemma 7 that $F \subseteq \mathcal{M}$.

(ii) Let $\mathcal{M}$ be a maximal ideal of $K[x, y]$ containing F, then by *(i)* there exists an $i \in \{1, \ldots, k\}$ such that $\langle G_i, H_i \rangle \subseteq \mathcal{M}$. Thus, $\mathcal{M}$ contains an irreducible factor $u(x)$ of G_i. Consider the canonical projection

$$\phi : \ K[x][y] \longrightarrow (K[x]/\langle u(x) \rangle)[y].$$

Let $L = K[x]/\langle u(x) \rangle$, Then $\phi(\mathcal{M})$ is a maximal ideal of $L[y]$, and $\phi(H_i) \in \phi(\mathcal{M})$. Therefore, $\phi(\mathcal{M})$ contains an irreducible factor α of $\phi(H_i)$. Choose $v(x, y) \in K[x, y]$ such that $\phi(v(x, y)) = \alpha$. Because $\langle u(x) \rangle \subseteq \mathcal{M}$, $v(x, y) \in \mathcal{M}$. Futhermore, $L[y]/\langle \phi(v(x, y)) \rangle$ is a field since $L[y]$ is a principal ideal domain and $\langle \phi(v(x, y)) \rangle$

is maximal. By the third isomorphism theorem, $L[y]/\langle\phi(v(x,y))\rangle$ is isomorphic to $K[x,y]/\langle u(x), v(x,y)\rangle$. Thus, $\langle u(x), v(x,y)\rangle$ is maximal and equals $\mathcal{M}$. □

The following remark serves to note an interesting fact about the common zeros of the f_i.

REMARK 1 *The set of common zeros of the f_i's equals the set of all (a,b) such that $\mathcal{M} = \langle x-a, y-b\rangle \supseteq F$.*

The reader should note that the condition in Theorem 3.2 that the f_i have no common factors implies that $\mathcal{I} = \langle f_0, \ldots, f_k\rangle$ is a zero dimensional ideal of $K[x,y]$; therefore, $\mathcal{I}$ has no embedded primes. Since every prime component of $\mathcal{I}$ is a maximal ideal, it can be computed by means of Theorem 3.2. The next example uses Theorem 3.2 to determine the maximal ideals containing the zero dimensional ideal generated by $F = \{f_0, f_1, f_2, f_3\} \in \mathbf{R}[x,y]$ of Example 3.1.

EXAMPLE 3.2 Let $\mathcal{I} = \langle f_0, f_1, f_2, f_3\rangle$ where

$$f_0 = x^7, \quad f_1 = y^2x^5 - yx^6, \quad f_2 = y^4x - y^3x^3, \quad f_3 = y^6 - y^5.$$

Recall $G_1 = x^2$, $G_2 = x^4$, $G_3 = x$, $H_1 = y^2 - yx$, $H_2 = y^4 - y^3x^2$, and $H_3 = y^6 - y^5$. Therefore, the maximal ideals containing $\mathcal{I}$ are

$$\mathcal{M}_1 = \langle x, y\rangle \quad \text{and} \quad \mathcal{M}_2 = \langle x, y-1\rangle$$

where $\langle G_1, H_1\rangle$, $\langle G_2, H_2\rangle$, $\langle G_3, H_3\rangle \subset \mathcal{M}_1$ and $\langle G_3, H_3\rangle \subset \mathcal{M}_2$.

The algorthm below computes a primary component of the zero dimensional ideal $\mathcal{I}$ for every maximal ideal containing $\mathcal{I}$.

ALGORITHM 3.1 *Let $\langle f_0, \ldots, f_k\rangle$ be a zero dimensional ideal of $K[x,y]$ given by a minimal Gröbner basis structured as in Theorem 3.1 with $PG_{k+1} = 1$, and let $\langle u(x), v(x,y)\rangle$ be a maximal ideal containing the f_i which is computed by means of Theorem 3.2.*

Input: $\langle f_0, \ldots, f_k \rangle$; $\langle u(x), v(x,y) \rangle$.

Output: A basis for the primary component of $\mathcal{I}$ corresponding to $\langle u(x), v(x,y) \rangle$.

Begin: *1.* REPLACE f_0 *by* $u(x)^m$

where m *is largest such that* $u(x)^m \mid f_0$.

2. Write H_k *as* $w(x,y)v(x,y)^n + z(x,y)u(x)$

where $v(x,y)$ *and* $w(x,y)$ *are relatively prime* mod $u(x)$.

Find $s \equiv v(x,y)^n \bmod u(x)$ *and* $t \equiv w(x,y) \bmod u(x)$

such that $H_k \equiv st \bmod u(x)^m$.

REPLACE H_k *by* s.

3. REMOVE *every* $f_i \in \{f_1, \ldots, f_{k-1}\}$

where $u(x)^m \mid f_i$ *or* $s \mid f_i$.

REMARK 2 *Theorem 3.2(ii) and Equation 3.3 imply that* H_k *can be written as described in the first part of step 2 above.*

To see how s and t are computed in step 2 of Algorithm 3.1, we consider the proposition below.

PROPOSITION 1 *Let* $R = K[x,y]$, *where* K *is a field. Let* $\mathcal{M} = \langle u(x), v(x,y) \rangle$ *be a maximal ideal of* R *where* $u(x)$ *is irreducible in* $K[x]$, *and* $v(x,y)$ *is irreducible over the field,* $L = K[x]/\langle u(x) \rangle$. *Let* $H \equiv v(x,y)^n w(x,y) \bmod u(x)$ *with* v *and* w *relatively prime* mod$u$. *Then for any integer* r, *there exist* $s_r(x,y)$ *and* $t_r(x,y)$ *so that* $s_r \equiv v^n \bmod u$ *and* $t_r \equiv w \bmod u$ *and* $H \equiv s_r t_r \bmod u^r$.

PROOF (Induction on r) If $r = 1$, by assumption, $s_1(x,y) = v(x,y)^n$ and $t_1(x,y) = w(x,y)$ will work. Assume true for r, i.e., $H \equiv s_r t_r \bmod u^r$ where $s_r \equiv v^n \bmod u$ and $t_r \equiv w \bmod u$. Thus, $H - s_r t_r \in \langle u^r \rangle$. Let $H - s_r t_r = u^r z$ where $z \in K[x,y]$. Since $s_r \equiv v^n \bmod u$ and $t_r \equiv w \bmod u$, $\bar{s_r} = \phi(s_r)$ and $\bar{t_r} = \phi(t_r)$ are relatively prime in $L[y]$, where ϕ is defined as in the proof of Theorem 3.2*(ii)*. So there exist $\bar{\alpha}$ and $\bar{\beta}$ such that

$$\bar{s_r}\bar{\alpha} + \bar{t_r}\bar{\beta} = 1$$

where $\bar{\alpha} \in L[y]$ and $\bar{\beta} \in L[y]$ can be found via the Euclidean algorithm. Now let $\phi(\alpha) = \bar{\alpha}$ and $\phi(\beta) = \bar{\beta}$, $s_{r+1} = s_r + \beta z u^r$, and $t_{r+1} = t_r + \alpha z u^r$. Clearly, $s_{r+1} \equiv s_r \bmod u$ and $t_{r+1} \equiv t_r \bmod u$. Now

$$s_{r+1}t_{r+1} = s_r t_r + (s_r\alpha + t_r\beta)zu^r + \alpha\beta z^2 u^{2r}.$$

However, $1 = \bar{s_r}\bar{\alpha} + \bar{t_r}\bar{\beta}$ so $s_r\alpha + t_r\beta = 1 + au$ for some $a \in K[x,y]$. Thus,

$$\begin{aligned} s_{r+1}t_{r+1} &= s_r t_r + (1+au)zu^r + \alpha\beta z^2 u^{2r} \\ &= s_r t_r + zu^r + azu^{r+1} + \alpha\beta z^2 u^{2r} \\ &= H + azu^{r+1} + \alpha\beta z^2 u^{2r}. \end{aligned}$$

Since $azu^{r+1} + \alpha\beta z^2 u^{2r} \in \langle u^{r+1} \rangle$, $H \equiv s_{r+1}t_{r+1} \bmod u^{r+1}$. □

Note that in the above proof, the induction step can be used as a subroutine in step 2 of Algorithm 3.1 to recursively obtain s_m and t_m where m is largest such that $u^m \mid f_0$.

The final theorem confirms that the primary decomposition of a zero dimensional ideal in $K[x,y]$ can be computed by means of the Algorithm 3.1.

THEOREM 3.3 *Let $\mathcal{I} = \langle f_0, \ldots, f_k \rangle$ where $F = \{f_0, \ldots, f_k\} \subset K[x,y]$ is a minimal Gröbner basis structured as in Theorem 3.1 and* $\gcd\{f_i\} = 1$. *The application of Algorithm 3.1 for each $\mathcal{M}$ computed in Theorem 3.2 yields the primary component for $\mathcal{M}$ in the primary decomposition of $\mathcal{I}$.*

PROOF Since $\mathcal{I}$ is a zero dimensional ideal in the Noetherian ring, $R = K[x,y]$, the minimal primes of $\mathcal{I}$ are maximal ideals, and so Theorem 1.6 and Corollary 1 of Theorem 1.7 imply that $\mathcal{I}$ has a unique irredundant primary decomposition, say

$$\mathcal{I} = \mathcal{Q}'_1 \cap \cdots \cap \mathcal{Q}'_r,$$

where for every $i = 1, \ldots, r$, $\sqrt{\mathcal{Q}'_i} = \mathcal{M}_i$, a maximal ideal containing $\mathcal{I}$. Hence $\mathcal{M}_i = \langle u, v \rangle$ where for some j, u is an irreducible factor of G_j and v is an irreducible

element of $(K[x]/\langle u\rangle)[y]$, as established in Theorem 3.2. It suffices to prove that the ith output $\mathcal{Q}_i$ is $\mathcal{M}_i$-primary and equals $\mathcal{Q}_i'$.

Fix i and let $\mathcal{M}_i = \mathcal{M} = \langle u, v\rangle$ be the ith input and $\mathcal{Q}_i = \mathcal{Q}$ the corresponding output. It is adequate to show that steps 1 and 2 of the algorithm produce the desired output since step 3 serves only to remove the f_i which are linear combinations of u^m and s and will clearly not change the ideal generated by $\{u^m, f_1, \ldots, f_{k-1}, s\}$. Therefore,

$$\mathcal{Q} = \langle u^m, f_1, \ldots, f_{k-1}, s\rangle,$$

where m and s are as described in Algorithm 3.1. Now the fact that

$$u^m \in \mathcal{Q} \qquad \text{and} \qquad s = v^n + qu \in \mathcal{Q}$$

implies that $v^{nm} = (s - qu)^m \in \mathcal{Q}$. Thus $\sqrt{\mathcal{Q}} \supseteq \mathcal{M}$ and since $\mathcal{M}$ is a maximal ideal, $\sqrt{\mathcal{Q}} = \mathcal{M}$ and Theorem 1.3 implies that $\mathcal{Q}$ is $\mathcal{M}$-primary.

To see that $\mathcal{Q} = \mathcal{Q}_i'$, we will first prove that $\mathcal{I}$, $\mathcal{Q}$, and $\mathcal{Q}_i'$ have the same localization at $\mathcal{M}$. First note that Theorem 1.10*(i)* yields $(\mathcal{Q}_j')_{\mathcal{M}} = R_{\mathcal{M}}$ for every $j \neq i$. Therefore,

$$\mathcal{I}_{\mathcal{M}} = (\mathcal{Q}_1')_{\mathcal{M}} \cap \cdots \cap (\mathcal{Q}_r')_{\mathcal{M}} = (\mathcal{Q}_i')_{\mathcal{M}}$$

follows from Theorem 1.11. Now $\mathcal{I} \subseteq \mathcal{Q}$, since

$$u^m \mid f_0 \qquad \text{and} \qquad f_k = H_k = st + pu^m$$

where t is as defined in Algorithm 3.1. Thus, $\mathcal{I}_{\mathcal{M}} \subseteq \mathcal{Q}_{\mathcal{M}}$. To verify $\mathcal{Q}_{\mathcal{M}} \subseteq \mathcal{I}_{\mathcal{M}}$, it is sufficient to show that u^m, $s \in \mathcal{I}_{\mathcal{M}}$ since $f_1, \ldots, f_{k-1}$ are clearly in $\mathcal{I}_{\mathcal{M}}$. Now $u^m \in \mathcal{I}_{\mathcal{M}}$ follows from the fact that m is greatest such that $u^m \mid f_0 \in K[x]$. Futhermore,

$$st = H_k - pu^m \in \mathcal{I}_{\mathcal{M}},$$

and by definition of t, $t \notin \mathcal{M}$. Therefore, $\dfrac{st}{t} = s \in \mathcal{I}_{\mathcal{M}}$, and thus $\mathcal{I}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} = (\mathcal{Q}_i')_{\mathcal{M}}$. Hence

$$\mathcal{Q}_i' = R \cap (\mathcal{Q}_i')_{\mathcal{M}} = R \cap \mathcal{Q}_{\mathcal{M}} = \mathcal{Q}$$

follows from Theorem 1.10*(ii)*. □

The following examples show applications of Algorithm 3.1. The first example refers back to F from Examples 3.1 and 3.2 where K is the field of real numbers.

EXAMPLE 3.3 Let $\mathcal{I} = \langle x^7, y^2x^5 - yx^6, y^4x - y^3x^3, y^6 - y^5 \rangle$ and recall

$$G_1 = x^2, \quad G_2 = x^4, \quad G_3 = x,$$

$$H_0 = 1, \quad H_1 = y^2 - yx, \quad H_2 = y^4 - y^3x^2, \quad H_3 = y^6 - y^5.$$

Therefore,

$$\mathcal{M}_1 = \langle x, y \rangle \quad \text{and} \quad \mathcal{M}_2 = \langle x, y - 1 \rangle.$$

The primary components for $\mathcal{I}$ are found by applying Algorithm 3.1 twice:

I. Input: $\mathcal{M}_1 = \langle x, y \rangle$.

1. No change since $f_0 = x^7$.
2. Replace H_3 with y^5 since x^7 does not divide $H_3 = y^5(y - 1)$.
3. No change since neither f_1 nor f_2 are divisible by f_0 or the new H_3.

Output: $\mathcal{Q}_1 = \langle x^7, f_1, f_2, y^5 \rangle$.

II. Input: $\mathcal{M}_2 = \langle x, y - 1 \rangle$.

1. No change.
2. Replace H_3 with $y - 1$ since x^7 does not divide $H_3 = y^5(y - 1)$.
3. No change since neither f_1 nor f_2 are divisible by f_0 or the new H_3.

Output: $\mathcal{Q}_2 = \langle x^7, f_1, f_2, y - 1 \rangle$.

Therefore, $\mathcal{I} = \langle x^7, y^2x^5 - yx^6, y^4x - y^3x^3, y^5 \rangle \cap \langle x^7, y^2x^5 - yx^6, y^4x - y^3x^3, y - 1 \rangle$ is the primary decomposition of $\mathcal{I}$.

EXAMPLE 3.4 Let $\mathcal{I} = \langle f_0, f_1, f_2 \rangle \in \mathbf{R}[x, y]$. where

$$f_0 = x^3 + x, \quad f_1 = yx^2 + y - x^2 - 1, \quad f_2 = y^2 - 2x^2 - 1.$$

Now $G_1 = x$, $G_2 = x^2 + 1$, $H_1 = y - 1$, $H_2 = y^2 - 2x^2 - 1$. Theorem 3.2 yields

$$\mathcal{M}_1 = \langle x, y - 1 \rangle, \quad \mathcal{M}_2 = \langle x^2 + 1, y - x \rangle, \quad \mathcal{M}_3 = \langle x^2 + 1, y + x \rangle$$

where $\mathcal{M}_1$ contains $\langle G_1, H_1 \rangle$, and $\mathcal{M}_2$ and $\mathcal{M}_3$ both contain $\langle G_2, H_2 \rangle$. The computation of the primary components is outlined below.

I. Input: $\mathcal{M}_1 = \langle x, y - 1 \rangle$.

1. Replace f_0 with x.
2. Replace H_2 with $y - 1$ since $H_2 = (y - 1)(y + 1) - 2x^2$.
3. Remove f_1 since $f_1 = (y - 1)(x^2 + 1)$.

Output: $\mathcal{Q}_1 = \langle x, y - 1 \rangle$.

II. Input: $\mathcal{M}_2 = \langle x^2 + 1, y - x \rangle$.

1. Replace f_0 with $x^2 + 1$.
2. Replace H_2 with $y - x$ since $H_2 = (y - x)(y + x) - (x^2 + 1)$.
3. Remove f_2.

Output: $\mathcal{Q}_2 = \langle x^2 + 1, y - x \rangle$.

III. Input: $\mathcal{M}_3 = \langle x^2 + 1, y + x \rangle$.

Output: $\mathcal{Q}_3 = \mathcal{M}_3$ is similar to II.

Thus, $\mathcal{I} = \langle x, y - 1 \rangle \cap \langle x^2 + 1, y - x \rangle \cap \langle x^2 + 1, y + x \rangle$ is the primary decomposition of $\mathcal{I}$.

As previously mentioned, Algorithm 3.1 is applicable only for zero dimensional ideals in $K[x,y]$. As discussed in Lazard (1985, p. 266), the one dimensional ideals of $K[x,y]$ can be dealt with by the algorithm after removing the greatest common divisor, PG_{k+1}, of the ideal's minimal Gröbner basis. Therefore, the prime components of the one dimensional ideals are the principal ideals generated by the irreducible factors of PG_{k+1} and the maximal ideals computed by means of Theorem 3.2 after removing PG_{k+1}. We can then use Algorithm 3.1 to compute the primary components of these maximal ideals, and then $\langle PG_{k+1}\rangle$ can be written as an intersection of primary ideals by factoring the generator to obtain a possibly nonstandard primary representation for a one dimensional ideal of $K[x,y]$.

The next example illustrates the use of Algorithm 3.1 for a one dimensional ideal.

EXAMPLE 3.5 Let $\mathcal{I} = \langle f_0, f_1, f_2\rangle \in \mathbf{R}[x,y]$ where

$$f_0 = yx^2(x^3 - 2x^2 + x), \quad f_1 = yx^2(xy^2 + 4xy + 4x),$$

$$f_2 = yx^2(y^3 + 12x^2y - 24xy - 16x^2 + 32x).$$

$\mathcal{I}$ is a one dimensional ideal since $\mathcal{I} \subset \langle y\rangle$. Also $D = \gcd\{f_i\} = yx^2$. Let $g_i = \frac{f_i}{D}$, then $\mathcal{J} = \langle g_0, g_1, g_2\rangle$ is a dimension zero ideal, and therefore, Algorithm 3.1 can be applied to the maximal ideals containing $\mathcal{J}$.

Now for $\mathcal{J}$,

$$G_1 = (x-1)^2, \quad G_2 = x, \quad H_1 = (y-2)^2, \quad H_2 = g_2 = y^3 + 12x^2y - 24xy - 16x^2 + 32x.$$

Then Theorem 3.2 yields

$$\mathcal{M}_1 = \langle x-1, y-2\rangle \supset \langle G_1, H_1\rangle, \quad \mathcal{M}_2 = \langle x, y\rangle \supset \langle G_2, H_2\rangle.$$

The computation of the primary components for $\mathcal{J}$ is as follows:

I. Input: $\mathcal{M}_1 = \langle x-1, y-2\rangle$.

1. Replace g_0 by $(x-1)^2$.

2. Replace h_2 by $(y-2)^2$ since $H_2 = (y-2)^2(y+4) + (12y-16)(x-1)^2$.

3. Remove g_1 since $(y-2)^2 \mid g_1 = x(y-2)^2$.

Output: $\mathcal{Q}_1 = \langle (x-1)^2, (y-2)^2 \rangle$.

II. Input: $\mathcal{M}_2 = \langle x, y \rangle$.

1. Replace f_0 by x since $g_0 = x(x-1)^2$.

2. Replace H_2 by y^3 since $H_2 = y^3 + x(12xy - 24y - 16x + 32)$.

3. Remove g_1 since $x \mid g_1 = x(y-2)^2$.

Output: $\mathcal{Q}_2 = \langle x, y^3 \rangle$.

Thus, $\mathcal{J} = \langle (x-1)^2, (y-2)^2 \rangle \cap \langle x, y^3 \rangle$ is the primary decomposition for $\mathcal{J}$. Now $\langle D \rangle = \langle y \rangle \cap \langle x^2 \rangle$ is the primary decomposition for $\langle D \rangle$. Therefore, we have

$$\mathcal{I} = (\langle y \rangle \cap \langle x^2 \rangle) \cdot (\langle (x-1)^2, (y-2)^2 \rangle \cap \langle x, y^3 \rangle),$$

as a decomposition for $\mathcal{I}$.

Note that in the above example, $\langle x \rangle$ and $\langle y \rangle$ are embedded prime ideals for $\mathcal{I}$ since $\langle x, y \rangle$ contains both $\langle x \rangle$ and $\langle y \rangle$. Therefore, the resulting decomposition is written as a product of two intersections of primary ideals. Note that if

$$A = \langle y \rangle \cap \langle x^2 \rangle \cap \langle (x-1)^2, (y-2)^2 \rangle \cap \langle x, y^3 \rangle$$

and

$$B = (\langle y \rangle \cap \langle x^2 \rangle) \cdot (\langle (x-1)^2, (y-2)^2 \rangle \cap \langle x, y^3 \rangle),$$

then $A \neq B$ since $x^2y(x-1)^2 \in A$, but $x^2y(x-1)^2 \notin B$.

In the next example, we look at a one dimensional ideal with no embedded components.

EXAMPLE 3.6 Let $\mathcal{I} = \langle f_0, f_1, f_2 \rangle$ where $f_i = (y-1)^2 g_i$ and the g_i are defined as in Example 3.5,

$$g_0 = x^3 - 2x^2 + x, \quad g_1 = xy^2 + 4xy + 4x, \quad g_2 = y^3 + 12x^2y - 24xy - 16x^2 + 32x.$$

As seen in Example 3.5, $\mathcal{J} = \langle (x-1)^2, (y-2)^2 \rangle \cap \langle x, y^3 \rangle$ is the primary decomposition for $\mathcal{J} = \langle g_0, g_1, g_2 \rangle$. Here $D = \gcd\{f_i\} = (y-1)^2$. Therefore, $\langle D \rangle = \langle (y-1)^2 \rangle$ and is not an embedded primary component for $\mathcal{I}$. Hence

$$\mathcal{I} = \langle (y-1)^2 \rangle \cap \langle (x-1)^2, (y-2)^2 \rangle \cap \langle x, y^3 \rangle.$$

And so we see that Algorithm 3.1 can produce a decomposition of any ideal in $K[x,y]$ once a minimal Gröbner basis for the ideal is computed. The decomposition will be the unique primary decomposition for the zero dimensional ideals of $K[x,y]$, but for one dimensional ideals, the primary decomposition may not be unique and may be a nonstandard decomposition involving a product of intersections of primary ideals.

Primary decomposition of ideals in $K[x,y]$ is just one of many applications of Gröbner bases. In addition to primary decomposition, Lazard (1985, pp. 267-270) applies Gröbner bases to resultants and Sylvester matrices. Buchberger (1985, pp. 200-222) shows applications of Gröbner bases to canonical simplification, to decisions of ideal congruence, to exact solutions of systems of algebraic equations, and to other related problems.

Bibliography

[1] Buchberger, B. (1985). Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. Chapter 6 in *Multidimensional Systems Theory*, N. K. Bose, editor. Dordrecht: Reidel.

[2] Burton, D. (1970). *A First Course in Rings and Ideals.* Reading, Mass: Addison-Wesley.

[3] Lazard, D. (1985). Ideal Bases and Primary Decomposition: Case of Two Variables. *J. Symbolic Computation, 1*, 261-270.

[4] Nagata, M. (1962). *Local Rings.* New York: Interscience.

[5] Northcott, D. (1968). *Lessons on Rings, Modules, and Multiplicities.* Cambridge: University Press.

[6] Robbiano, L. (n.d.). Gröbner Bases: A Foundation for Commutative Algebra. Preprint.

[7] Zariski, O. & Samuel, P. (1958). *Commutative Algebra. Vol. 1.* Princeton: Van Nostrand.